DOCKET NO.: 255635US6PCT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Satoshi KITANI, et al.

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HEREWITH

INTERNATIONAL APPLICATION NO.: PCT/JP03/16226

INTERNATIONAL FILING DATE: December 18, 2003

FOR: MUTUALLY AUTHENTICATING METHOD, PROGRAM, RECORDING MEDIUM, SIGNAL PROCESSING SYSTEM, REPRODUCING APPARATUS, AND INFORMATION PROCESSING APPARATUS

REQUEST FOR PRIORITY UNDER 35 U.S.C. 119 AND THE INTERNATIONAL CONVENTION

Commissioner for Patents
Alexandria, Virginia 22313

Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

COUNTRY	APPLICATION NO	DAY/MONTH/YEAR
Japan	2003-006915	15 January 2003

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/JP03/16226. Receipt of the certified copy(s) by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

Respectfully submitted,
OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Gregory J. Maier
Attorney of Record
Registration No. 25,599
Surinder Sachar
Registration No. 34,423

Customer Number
22850

(703) 413-3000
Fax No. (703) 413-2220
(OSMMN 08/03)

S04P0076WWUUU

PCT/JP03/16226

Rec'd PCT/PTO 31 AUG 2004

18.12.03

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　１月１５日

出願番号
Application Number: 特願２００３－００６９１５

[ST. 10/C]: [ＪＰ２００３－００６９１５]

出願人
Applicant(s): ソニー株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

２００３年１１月　７日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００３－３０９２３０９

【書類名】　特許願
【整理番号】　0290782806
【提出日】　平成15年 1月15日
【あて先】　特許庁長官　太田　信一郎　殿
【国際特許分類】　H04N　5/85
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　木谷　聡
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　村松　克美
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
【代理人】
　【識別番号】　100082762
　【弁理士】
　【氏名又は名称】　杉浦　正知
　【電話番号】　03-3980-0339
【選任した代理人】
　【識別番号】　100120640
　【弁理士】
　【氏名又は名称】　森　幸一
【手数料の表示】
　【予納台帳番号】　043812
　【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0201252

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　相互認証方法、プログラム、記録媒体、信号処理システム、再生装置および情報処理装置

【特許請求の範囲】

【請求項１】　不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、上記再生装置が上記コンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置と相互に認証する相互認証方法において、

上記再生装置は、当該再生装置を表す情報と上記リボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第１の判定ステップを有し、

上記情報処理装置は、当該情報処理装置を表す情報と上記リボケーション情報を用いて当該情報処理装置を無効化すべきか否かを判定する第２の判定ステップを有し、

上記第１の判定手段によって無効化すべきという判定をされなかった場合に生成される第１の鍵情報と、上記第２の判定手段によって無効化すべきという判定をされなかった場合に生成される第２の鍵情報とを用いて、上記再生装置と上記情報処理装置とが相互に認証する相互認証ステップとを有することを特徴とする相互認証方法。

【請求項２】　請求項１において、

上記相互認証ステップは、

上記情報処理装置が上記伝達手段を介して正常に動作しているかを上記再生装置において確認する第１の確認ステップと、

上記再生装置が上記伝達手段を介して正常に動作しているかを上記情報処理装置において確認する第２の確認ステップとを有することを特徴とする請求項１に記載の相互認証方法。

【請求項３】　請求項２において、

上記再生装置は、

乱数を生成する第１の乱数生成ステップと、

所定の計算をする第１の計算ステップとを有し、

上記情報処理装置は、

乱数を生成する第２の乱数生成ステップと、

所定の計算をする第２の計算ステップとを有し、

上記第１の確認ステップは、

上記第１の乱数生成ステップにより生成される第１の乱数と、上記第２の乱数生成ステップにより生成される第２の乱数とを上記伝達手段を介して上記再生装置と上記情報処理装置との間で相互に交換する第１の乱数交換ステップと、

上記再生装置において、少なくとも上記第１の鍵情報と上記相互に交換された第１の乱数および第２の乱数とを用いて上記第１の計算ステップにより計算した結果と、上記情報処理装置から上記伝達手段を介して送られた、少なくとも上記第２の鍵情報と上記相互に交換された第１の乱数および第２の乱数とを用いて上記第２の計算ステップにより計算した結果とが同一であるかを比較する第１の比較ステップとを有し、

上記第２の確認ステップは、

上記第１の乱数生成ステップにより生成される第３の乱数と、上記第２の乱数生成ステップにより生成される第４の乱数とを上記伝達手段を介して上記再生装置および上記情報処理装置との間で相互に交換する第２の乱数交換ステップと、

上記情報処理装置において、上記再生装置から上記伝達手段を介して送られた、少なくとも上記第１の鍵情報と上記相互に交換された第３の乱数および第４の乱数とを用いて上記第１の計算ステップにより計算した結果と、少なくとも上記第２の鍵情報と上記相互に交換された第３の乱数および第４の乱数とを用いて上記第２の計算ステップにより計算した結果とが同一であるかを比較する第２の比較ステップとを有していることを特徴とする相互認証方法。

【請求項４】　不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、上記再生装置が上記コンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置と相互に認証する相互認証方法のプログラムであって、

上記再生装置は、当該再生装置を表す情報と上記リボケーション情報とを用い

て当該再生装置を無効化すべきか否かを判定する第１の判定ステップを有し、

上記情報処理装置は、当該情報処理装置を表す情報と上記リボケーション情報を用いて当該情報処理装置を無効化すべきか否かを判定する第２の判定ステップを有し、

上記第１の判定手段によって無効化すべきという判定をされなかった場合に生成される第１の鍵情報と、上記第２の判定手段によって無効化すべきという判定をされなかった場合に生成される第２の鍵情報とを用いて、上記再生装置と上記情報処理装置とが相互に認証する相互認証ステップとを有することを特徴とする相互認証方法のプログラム。

【請求項５】　不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、上記再生装置が上記コンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置と相互に認証する相互認証方法のプログラムを格納した記録媒体であって、

上記再生装置は、当該再生装置を表す情報と上記リボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第１の判定ステップを有し、

上記情報処理装置は、当該情報処理装置を表す情報と上記リボケーション情報を用いて当該情報処理装置を無効化すべきか否かを判定する第２の判定ステップを有し、

上記第１の判定手段によって無効化すべきという判定をされなかった場合に生成される第１の鍵情報と、上記第２の判定手段によって無効化すべきという判定をされなかった場合に生成される第２の鍵情報とを用いて、上記再生装置と上記情報処理装置とが相互に認証する相互認証ステップとを有することを特徴とする相互認証方法のプログラムを格納した記録媒体。

【請求項６】　不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、上記再生装置が上記コンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置とを備える信号処理システムであって、

上記再生装置は、当該再生装置を表す情報と上記リボケーション情報とを用い

て当該再生装置を無効化すべきか否かを判定する第１の判定手段を有し、

上記情報処理装置は、当該情報処理装置を表す情報と上記リボケーション情報とを用いて当該情報処理装置を無効化すべきか否かを判定する第２の判定手段を有し、

上記第１の判定手段によって無効化すべきという判定をされなかった場合に生成される第１の鍵情報と、上記第２の判定手段によって無効化すべきという判定をされなかった場合に生成される第２の鍵情報とを用いて、上記再生装置と上記情報処理装置とが相互に認証する相互認証手段と、

上記相互認証手段による相互認証後に、上記再生装置および上記情報処理装置に共通の共通鍵を生成する共通鍵生成手段とを備えることを特徴とする信号処理システム。

【請求項７】　請求項６において、

上記相互認証手段は、

上記情報処理装置が上記伝達手段を介して正常に動作しているかを上記再生装置において確認する第１の確認手段と、

上記再生装置が上記伝達手段を介して正常に動作しているかを上記情報処理装置において確認する第２の確認手段とを有することを特徴とする信号処理システム。

【請求項８】　請求項７において、

上記再生装置は、

乱数を生成する第１の乱数生成手段と、

所定の計算をする第１の計算手段とを有し、

上記情報処理装置は、

乱数を生成する第２の乱数生成手段と、

所定の計算をする第２の計算手段とを有し、

上記第１の確認手段は、

上記第１の乱数生成手段により生成される第１の乱数と、上記第２の乱数生成手段により生成される第２の乱数とを上記伝達手段を介して上記再生装置と上記情報処理装置との間で相互に交換する第１の乱数交換手段と、

上記再生装置において、少なくとも上記第１の鍵情報と上記相互に交換された第１の乱数および第２の乱数とを用いて上記第１の計算手段により計算した結果と、上記情報処理装置から上記伝達手段を介して送られた、少なくとも上記第２の鍵情報と上記相互に交換された第１の乱数および第２の乱数とを用いて上記第２の計算手段により計算した結果とが同一であるかを比較する第１の比較手段とを有し、

上記第２の確認手段は、

上記第１の乱数生成手段により生成される第３の乱数と、上記第２の乱数生成手段により生成される第４の乱数とを上記伝達手段を介して上記再生装置および上記情報処理装置との間で相互に交換する第２の乱数交換手段と、

上記情報処理装置において、上記再生装置から上記伝達手段を介して送られた、少なくとも上記第１の鍵情報と上記相互に交換された第３の乱数および第４の乱数とを用いて上記第１の計算手段により計算した結果と、少なくとも上記第２の鍵情報と上記相互に交換された第３の乱数および第４の乱数とを用いて上記第２の計算手段により計算した結果とが同一であるかを比較する第２の比較手段とを有していることを特徴とする信号処理システム。

【請求項９】　請求項８において、

上記共通鍵生成手段は、

上記第１の乱数生成手段により生成される第５の乱数と、上記第２の乱数生成手段により生成される第６の乱数とを上記伝達手段を介して上記再生装置と上記情報処理装置との間で相互に交換する第３の乱数交換手段と、

上記再生装置において、少なくとも上記第１の鍵情報と上記第５の乱数と上記第６の乱数とを用いて上記共通鍵を生成する第１の共通鍵生成手段と、

上記情報処理装置において、少なくとも上記第２の鍵情報と上記第５の乱数と上記第６の乱数とを用いて上記共通鍵を生成する第２の共通鍵生成手段とを有することを特徴とする信号処理システム。

【請求項１０】　請求項９において、

上記伝達手段を介して、上記共通鍵を用いた共通鍵暗号方式で上記再生装置から上記情報処理装置へ情報を送る第１の送信手段と、

上記再生装置において、上記第１の鍵情報と上記記録媒体固有の情報を用いて記録媒体固有の鍵情報を生成する中間鍵情報生成手段とを備えることを特徴とする請求項７に記載の信号処理システム。

【請求項１１】　請求項１０において、

第３の鍵情報を、少なくとも上記記録媒体固有の鍵情報を用いて暗号化する鍵情報暗号化手段と、

上記鍵情報暗号化手段により暗号化された上記第３の鍵情報を上記記録媒体に記録する暗号化鍵情報記録手段と、

上記第３の鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成手段と、

上記コンテンツ情報暗号化鍵を用いて暗号化されたコンテンツ情報を上記記録媒体に記録するコンテンツ情報記録手段とを備えることを特徴とする信号処理システム。

【請求項１２】　請求項１１において、

上記鍵情報暗号化手段、上記暗号化鍵情報記録手段、上記最終暗号化鍵生成手段、上記コンテンツ情報記録手段は、

上記情報処理装置が有しているとともに、

上記記録媒体固有の鍵情報は、

上記第１の送信手段により上記情報処理装置へ送られることを特徴とする信号処理システム。

【請求項１３】　請求項１２において、

上記第３の鍵情報は、

上記再生装置において前期第１の乱数生成手段により生成された第７の乱数に基づいた鍵情報であるとともに、

当該第３の鍵情報は、

上記第１の送信手段により上記情報処理装置に送られることを特徴とする信号処理システム。

【請求項１４】　請求項１２において、

上記第３の鍵情報は、

上記情報処理装置において上記第２の乱数生成手段により生成された第８の乱数に基づいた鍵情報であることを特徴とする信号処理システム。

【請求項１５】　請求項１１において、

上記鍵情報暗号化手段、上記暗号化鍵情報記録手段、上記コンテンツ情報記録手段は、　上記情報処理装置が有しており、

上記記録媒体固有の鍵情報は、

上記第１の送信手段により上記情報処理装置へ送られるとともに、

上記最終暗号化鍵生成手段は、

上記再生装置が有しており、

上記最終暗号化鍵生成手段により生成された上記コンテンツ情報暗号化鍵は、

上記第１の送信手段により上記情報処理装置へ送られることを特徴とする信号処理システム。

【請求項１６】　請求項１５において、

上記第３の鍵情報は、

上記再生装置において上記第１の乱数生成手段により生成された第９の乱数を基にした鍵情報であることを特徴とする請求項１３に記載の信号処理システム。

【請求項１７】　請求項１５において、

上記第３の鍵情報は、

上記情報処理装置において上記第２の乱数生成手段により生成された第１０の乱数を基にした鍵情報であるとともに、

上記伝達手段を介して、上記共通鍵を用いた共通鍵暗号方式で上記情報処理装置から上記再生装置へ情報を送る第２の送信手段により上記再生装置の上記最終暗号化鍵生成手段に送られることを特徴とする信号処理システム。

【請求項１８】　請求項１０において、

上記記録媒体から読み出される暗号化された第４の鍵情報を、少なくとも上記記録媒体固有の鍵情報を用いて復号する鍵情報復号手段と、

上記第４の鍵情報に基づいてコンテンツ情報復号鍵を生成する最終復号鍵生成手段と、　上記コンテンツ情報復号鍵を用いて上記コンテンツ情報を復号するコンテンツ情報復号手段とを備えていることを特徴とする信号処理システム。

【請求項１９】　請求項１８において、
上記最終復号鍵生成手段、上記コンテンツ情報復号手段は、
上記情報処理装置が有していることを特徴とする信号処理システム。
【請求項２０】　請求項１９において、
上記鍵情報復号手段は、
上記情報処理装置が有しており、
上記記録媒体固有の鍵情報は、
上記第１の送信手段によって上記情報処理装置へ送られることを特徴とする信号処理システム。
【請求項２１】　請求項１９において、
上記鍵情報復号手段は、
上記再生装置が有しており、
復号された上記第４の鍵情報は、
上記第１の送信手段によって上記情報処理装置へ送られることを特徴とする信号処理システム。
【請求項２２】　請求項１８において、
上記最終復号鍵生成手段は、
上記再生装置が有していることを特徴とする信号処理システム。
【請求項２３】　請求項２２において、
上記鍵情報復号手段は、
上記再生装置が有しており、
上記再生装置において生成された上記コンテンツ情報復号鍵は、
上記第１の送信手段によって上記情報処理装置へ送られることを特徴とする信号処理システム。
【請求項２４】　不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有し、上記コンテンツ情報が伝達手段を介して情報処理装置に送信され、処理される信号処理システムにおける再生装置であって、
当該再生装置を表す情報と上記リボケーション情報とを用いて当該再生装置を

無効化すべきか否かを判定する第１の判定手段を有し、

上記第１の判定手段によって無効化すべきという判定をされなかった場合に生成される第１の鍵情報と、

上記情報処理装置に設けられている当該情報処理装置を表す情報と上記リボケーション情報とを用いて当該情報処理装置を無効化すべきか否かを判定する第２の判定手段によって無効化すべきという判定をされなかった場合に生成される第２の鍵情報とを用いて、上記情報処理装置と相互に認証する相互認証手段と、

上記相互認証手段による相互認証後に、上記情報処理装置と共通の共通鍵を生成する共通鍵生成手段とを備えることを特徴とする再生装置。

【請求項２５】　不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、再生装置がコンテンツ情報を読み出し、上記コンテンツ情報が伝達手段を介して受信され、処理される情報処理装置であって、

上記再生装置に設けられている第１の判定手段によって、当該再生装置を表す情報と上記リボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定し、上記第１の判定手段によって無効化すべきという判定をされなかった場合に生成される第１の鍵情報と、

当該情報処理装置を表す情報と上記リボケーション情報とを用いて当該情報処理装置を無効化すべきか否かを判定する第２の判定手段を有し、

上記第１の鍵情報と、上記第２の判定手段によって無効化すべきという判定をされなかった場合に生成される第２の鍵情報とを用いて、上記再生装置と相互に認証する相互認証手段と、

上記相互認証手段による相互認証後に、上記再生装置と共通の共通鍵を生成する共通鍵生成手段とを備えることを特徴とする情報処理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、例えばパーソナルコンピュータと接続されたドライブによってディスクメディアに暗号化コンテンツを記録し、また、ディスクメディアから暗号

化コンテンツを再生する場合に適用される相互認証方法、プログラム、記録媒体、信号処理システム、再生装置および情報処理装置に関する。

【０００２】

【従来の技術】

近年開発されたＤＶＤ(Digital Versatile Disc またはDigital Video Disc)等の記録媒体では、１枚の媒体に例えば映画１本分の大量のデータをディジタル情報として記録することが可能である。このように映像情報等をディジタル情報として記録することが可能となってくると不正コピーを防止して著作権の保護を図ることがますます重要となっている。

【０００３】

ＤＶＤ－Videoでは、コピープロテクション技術としてＣＳＳ(Content Scrambling System)が採用されている。ＣＳＳは、ＤＶＤ－ＲＯＭメディアに対する適用のみが認可されており、ＤＶＤ－Ｒ、ＤＶＤ－ＲＷ、ＤＶＤ＋Ｒ、ＤＶＤ＋ＲＷ等の記録型ＤＶＤでのＣＳＳの利用がＣＳＳ契約によって禁止されている。したがって、ＣＳＳ方式で著作権保護されたＤＶＤ－Videoの内容を記録型ＤＶＤへのまるごとコピー（ビットバイビットコピー）することは、ＣＳＳ契約上では、認められた行為ではない。

【０００４】

しかしながら、ＣＳＳの暗号方式が破られる事態が発生した。ＣＳＳの暗号化を解除してＤＶＤ－Videoの内容を簡単にハードディスクにコピーすることを可能とする「ＤｅＣＳＳ」と呼ばれるソフトウェアがインターネット上で配布された。「ＤｅＣＳＳ」が出現した背景には、本来耐タンパー化が義務付けられているはずのＣＳＳ復号用の鍵データを耐タンパー化しないまま設計された再生ソフトウェアがリバースエンジニアされて鍵データが解読されたことによって、連鎖的にＣＳＳアルゴリズム全体が解読された経緯がある。

【０００５】

ＣＳＳの後に、ＤＶＤ－Audio等のＤＶＤ－ＲＯＭの著作権保護技術であるＣＰＰＭ(Content Protection for Pre-Recorded Media)、並びに記録型ＤＶＤ、メモリカードに関する著作権保護技術ＣＰＲＭ(Content Protection for Record

able Media）が提案されている。これらの方式は、コンテンツの暗号化や管理情報の格納等に問題が生じたときに、システムを更新でき、また、データをまるごとコピーしても再生を制限できる特徴を有している。ＤＶＤに関する著作権保護の方法に関しては、下記の非特許文献１に説明され、ＣＰＲＭは、ライセンス管理者である米4C Entity,LLCが配布する下記の資料（非特許文献２）に説明されている。

【０００６】

【非特許文献１】

山田，「ＤＶＤを起点に著作権保護空間を広げる」，日経エレクトロニクス 2001.8.13,p.143-153

【０００７】

【非特許文献２】

"Content Protection for Recordable Media Specification DVD Book"、インターネット＜ＵＲＬ：http://www.4Centity.com/＞

【０００８】

【発明が解決しようとする課題】

パーソナルコンピュータ（以下、適宜ＰＣと略す）環境下では、ＰＣとドライブとが標準的インターフェースで接続されるために、標準的インターフェースの部分で秘密保持が必要なデータが知られたり、データが改ざんされるおそれがある。また、アプリケーションソフトウェアがリバースエンジニアリングされ、秘密情報が盗まれたり、改ざんされる危険がある。このような危険性は、記録再生装置が一体に構成された電子機器の場合では、生じることが少ない。

【０００９】

著作権保護技術をＰＣ上で実行されるアプリケーションプログラムへ実装する際には、その著作権保護技術の解析を防ぐため耐タンパー性を持たせるのが一般的である。しかしながら、耐タンパー性の強度を示す指標がなく、その結果、どの程度のリバースエンジニアリングへの対応を行うかは、インプレメンターの個々の判断や能力に委ねられているのが現状である。ＣＳＳの場合は、結果としてその著作権保護技術が破られてしまった。さらに、ＣＳＳの後に提案されたＣＰ

ＰＭおよび記録型ＤＶＤに関する著作権保護技術ＣＰＲＭにおいても、既に破られているＣＳＳに新たな機能を加えたものであり、また、著作権保護技術に関わるアルゴリズムは、大部分がＰＣでの実装に依存するものであり、コンテンツプロテクションの機能が充分に強いものと言えない問題があった。すなわち、アプリケーションソフトウェアなどのリバースエンジニアリングによって、著作権保護技術に関わる秘密情報の解析により暗号方式が破られ、ディスクからのデータとしてＰＣがそのまま読み出した暗号化コンテンツが「ＤｅＣＳＳ」のような解読ソフトウェアにより復号され、平文のままのクリア・コンテンツとしてコピー制限の働かない状態で複製が繰り返されるような事態を招くことで、著作権保護が機能しなくなるという危険性があった。

【００１０】

したがって、この発明の目的は、ＰＣ環境下でも著作権保護技術の安全性を確保することができる相互認証方法、プログラム、記録媒体、信号処理システム、再生装置および情報処理装置を提供することにある。

【００１１】

【課題を解決するための手段】

上述した課題を解決するために、請求項１の発明は、不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、再生装置がコンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置と相互に認証する相互認証方法において、

再生装置は、当該再生装置を表す情報とリボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第１の判定ステップを有し、

情報処理装置は、当該情報処理装置を表す情報とリボケーション情報を用いて当該情報処理装置を無効化すべきか否かを判定する第２の判定ステップを有し、

第１の判定手段によって無効化すべきという判定をされなかった場合に生成される第１の鍵情報と、第２の判定手段によって無効化すべきという判定をされなかった場合に生成される第２の鍵情報とを用いて、再生装置と情報処理装置とが相互に認証する相互認証ステップとを有することを特徴とする相互認証方法であ

る。

【００１２】

請求項４の発明は、不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、再生装置がコンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置と相互に認証する相互認証方法のプログラムであって、

再生装置は、当該再生装置を表す情報とリボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第１の判定ステップを有し、

情報処理装置は、当該情報処理装置を表す情報とリボケーション情報を用いて当該情報処理装置を無効化すべきか否かを判定する第２の判定ステップを有し、

第１の判定手段によって無効化すべきという判定をされなかった場合に生成される第１の鍵情報と、第２の判定手段によって無効化すべきという判定をされなかった場合に生成される第２の鍵情報とを用いて、再生装置と情報処理装置とが相互に認証する相互認証ステップとを有することを特徴とする相互認証方法のプログラムである。

【００１３】

請求項５の発明は、不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、再生装置がコンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置と相互に認証する相互認証方法のプログラムを格納した記録媒体であって、

再生装置は、当該再生装置を表す情報とリボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第１の判定ステップを有し、

情報処理装置は、当該情報処理装置を表す情報とリボケーション情報を用いて当該情報処理装置を無効化すべきか否かを判定する第２の判定ステップを有し、

第１の判定手段によって無効化すべきという判定をされなかった場合に生成される第１の鍵情報と、第２の判定手段によって無効化すべきという判定をされなかった場合に生成される第２の鍵情報とを用いて、再生装置と情報処理装置とが相互に認証する相互認証ステップとを有することを特徴とする相互認証方法のプ

ログラムを格納した記録媒体である。

【００１４】

請求項６の発明は、不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、再生装置がコンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置とを備える信号処理システムであって、

再生装置は、当該再生装置を表す情報とリボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第１の判定手段を有し、

情報処理装置は、当該情報処理装置を表す情報とリボケーション情報とを用いて当該情報処理装置を無効化すべきか否かを判定する第２の判定手段を有し、

第１の判定手段によって無効化すべきという判定をされなかった場合に生成される第１の鍵情報と、第２の判定手段によって無効化すべきという判定をされなかった場合に生成される第２の鍵情報とを用いて、再生装置と情報処理装置とが相互に認証する相互認証手段と、

相互認証手段による相互認証後に、再生装置および情報処理装置に共通の共通鍵を生成する共通鍵生成手段とを備えることを特徴とする信号処理システムである。

【００１５】

請求項２４の発明は、不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有し、コンテンツ情報が伝達手段を介して情報処理装置に送信され、処理される信号処理システムにおける再生装置であって、

当該再生装置を表す情報とリボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第１の判定手段を有し、

第１の判定手段によって無効化すべきという判定をされなかった場合に生成される第１の鍵情報と、

情報処理装置に設けられている当該情報処理装置を表す情報とリボケーション情報とを用いて当該情報処理装置を無効化すべきか否かを判定する第２の判定手段によって無効化すべきという判定をされなかった場合に生成される第２の鍵情

報とを用いて、情報処理装置と相互に認証する相互認証手段と、

相互認証手段による相互認証後に、情報処理装置と共通の共通鍵を生成する共通鍵生成手段とを備えることを特徴とする再生装置である。

【００１６】

請求項２５の発明は、不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、再生装置がコンテンツ情報を読み出し、コンテンツ情報が伝達手段を介して受信され、処理される情報処理装置であって、

再生装置に設けられている第１の判定手段によって、当該再生装置を表す情報とリボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定し、第１の判定手段によって無効化すべきという判定をされなかった場合に生成される第１の鍵情報と、

当該情報処理装置を表す情報とリボケーション情報とを用いて当該情報処理装置を無効化すべきか否かを判定する第２の判定手段を有し、

第１の鍵情報と、第２の判定手段によって無効化すべきという判定をされなかった場合に生成される第２の鍵情報とを用いて、再生装置と相互に認証する相互認証手段と、

相互認証手段による相互認証後に、再生装置と共通の共通鍵を生成する共通鍵生成手段とを備えることを特徴とする情報処理装置である。

【００１７】

この発明では、メディア上に記録された鍵情報（ＭＫＢ）と各デバイスまたは各アプリケーションに記憶されている鍵情報（デバイスキー）から同一の値として導かれる鍵情報（メディアキー）を利用して相互認証がなされる。したがって、この発明においては、認証のためだけに用意される特定の認証鍵を必要とせず、秘密情報を少なくでき、また、デバイスまたはアプリケーションによってデバイスキーを異ならせることが可能であるので、秘密情報が不正に読み取られる危険性を少なくできる。また、この発明では、著作権保護技術に関する秘密情報である電子機器またはアプリケーションソフトウェア固有の情報例えばデバイスキーがドライブ内に実装されているので、情報処理装置にインストールされるアプ

リケーションソフトウェアは、著作権保護技術に関する秘密情報の全てを持つ必要がなくなる。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

【００１８】

また、電子機器固有の情報としてのデバイスキーを記録再生装置が持つことによって、記録再生装置自身をリボークすることが可能となる。さらに、この発明では、情報処理装置におけるコンテンツキーを計算するのに必要とされる乱数情報が記録再生装置内の例えばＬＳＩによって生成できるので、ＰＣ内でソフトウェアによって乱数を生成するのと比較して、真正または真正乱数に近い乱数を生成することができる。したがって、乱数が固定値に置き換えられる、等のおそれを少なくできる。

【００１９】

【発明の実施の形態】

この発明の一実施形態の説明に先立って、本明細書の特許請求の範囲において使用される用語と実施の形態中で使用される用語との対応関係について以下に説明する。

【００２０】

記録媒体：メディア例えばディスク、再生装置：ドライブ、情報処理装置：ホスト、伝達手段：ドライブーホストインターフェース、信号処理システム：メディアを再生するドライブとホストとがドライブーホストインターフェースを介して接続されるシステムである。第１の送信手段：ドライブ側からセッションキーを共通鍵とした共通鍵暗号方式で情報をホスト側に送る手段、第２の送信手段：逆にホスト側からセッションキーを共通鍵として情報をドライブ側に送る手段のことである。

【００２１】

コンテンツ情報：メディアに記録されている情報または記録すべき情報をコンテンツ情報としている。リボケーション情報：メディアに予め記録されているメディアキーブロックＭＫＢ(Media Key Blocks)、記録媒体固有の情報：メディア

ＩＤ、デバイスキー：再生装置または情報処理装置を表す情報、装置を無効化すべきか否かを判定する判定手段：プロセスＭＫＢである。プロセスＭＫＢでは、ドライブ側の第１の判定手段によりドライブが無効化されなければ、ドライブ側のメディアキーとして第１の鍵情報が生成され、ホスト側の第２の判定手段によりホストが無効化されなければ、ホスト側のメディアキーとして第２の鍵情報が生成される。ドライブとホストは、独立して無効化が可能であり、無効化された場合は、期待されるメディアキーを得ることができないので「第１の」、「第２の」と分けている。

【００２２】

相互認証手段：ＡＫＥ(Authentication and Key Exchange)（プロセスＭＫＢ以降の乱数交換、ＭＡＣ計算、比較からなるドライブ側の第１の確認手段とホスト側の第２の確認手段により相互に相手の動作を確認することである。ドライブ側とホスト側の何れが先に確認するかの順番は、任意であるので、用語の統一を図るために、ドライブ側の確認手段を「第１の」としている。）

【００２３】

共通鍵：セッションキー（確実に暗号化・復号に使われるセッションキーとコンテンツキーとは、「鍵」でそれ以外は「鍵情報」としている。認証完了後なので共通鍵として同じ暗号化鍵が生成されるが、生成している装置と、基にしている鍵情報の呼び方を変えていることから、ドライブ側の生成手段を第１の共通鍵生成手段、ホスト側の生成手段を第２の共通鍵生成手段としている。）

【００２４】

乱数を生成する乱数生成手段：乱数発生器（ＲＮＧ：Random Number Generator)（ドライブ側の乱数生成手段を第１の乱数生成手段、ホスト側の乱数生成手段を第２の乱数生成手段とし、特許請求の範囲においては、生成される乱数に対して請求項に出てくる順番で番号をつけている。）

【００２５】

所定の計算を行う計算手段：ＭＡＣ(Message Authentication Code)演算ブロック（乱数交換手段により交換された乱数を用いて、ドライブ側で計算する手段を第１の計算手段、ホスト側の計算手段を第２の計算手段としている。）

【００２６】

比較手段：比較（ドライブ側の比較を第１の比較手段、ホスト側の比較を第２の比較手段としている。）

【００２７】

記録媒体固有の鍵情報：メディアユニークキー（本実施形態においては、メディアユニークキーの生成は耐タンパー性を持たせるために全てドライブ側で行われているので、記録媒体固有の鍵情報（メディアユニークキー）を生成する中間鍵生成手段は、ドライブ側のみとしている。）

【００２８】

コンテンツ情報暗号化鍵またはコンテンツ情報復号鍵の基になる鍵情報：（記録時に使われるタイトルキーを第３の鍵情報、再生時に使われるタイトルキーを第４の鍵情報としている。また、メディアユニークキーによってタイトルキーを暗号化する手段を鍵情報暗号化手段、復号する手段を鍵情報復号手段としている。メディアユニークキーによって暗号化されたタイトルキーを記録媒体に記録する手段を暗号化鍵情報記録手段としている。）

【００２９】

コンテンツ情報を暗号化または復号するための鍵：コンテンツキー（記録時に使われるコンテンツキーをコンテンツ情報暗号化鍵とし、再生時に使われるコンテンツキーをコンテンツ情報復号鍵としている。コンテンツ情報暗号化鍵を生成する手段を最終暗号化鍵生成手段、コンテンツ情報復号鍵を生成する手段を最終復号鍵生成手段としている。暗号化されたコンテンツ情報を記録媒体に記録する手段をコンテンツ情報記録手段とし、暗号化されたコンテンツ情報を復号する手段をコンテンツ情報復号手段としている。）

【００３０】

次に、この発明の理解の容易のために、最初に図１を参照して著作権保護技術例えばＤＶＤ用ＣＰＲＭのアーキテクチャについて説明する。図１において、参照符号１が例えばＣＰＲＭ規格に準拠したＤＶＤ－Ｒ／ＲＷ、ＤＶＤ－ＲＡＭ等の記録型ＤＶＤメディアを示し、参照符号２が例えばＣＰＲＭ規格に準拠したレコーダを示し、参照符号３が例えばＣＰＲＭ規格に準拠したプレーヤを示す。レ

コーダ２およびプレーヤ３は、機器またはアプリケーションソフトウェアである。

【００３１】

未記録ディスクの状態において、ＤＶＤメディア１の最内周側のリードインエリアのＢＣＡ(Burst Cutting Area)またはＮＢＣＡ(Narrow Burst Cutting Area)と称されるエリアには、メディアＩＤ１１が記録され、リードインエリアのエンボスまたはプリ記録データゾーンには、メディアキーブロック（以下、ＭＫＢと適宜略す）１２が予め記録されている。メディアＩＤ１１は、個々のメディア単位例えばディスク１枚毎に異なる番号であり、メディアの製造者コードとシリアル番号から構成される。メディアＩＤ１１は、メディアキーを個々のメディアで異なるメディアユニークキーへ変換する際に必要となる。メディアキーブロックＭＫＢは、メディアキーの導出、並びに機器のリボケーション（無効化）を実現するための鍵束である。これらのメディアＩＤおよびメディアキーブロックは、記録媒体固有の第１の情報である。

【００３２】

ディスク１の書き換えまたは追記可能なデータ領域には、コンテンツキーで暗号化された暗号化コンテンツ１３が記録される。暗号化方式としては、Ｃ２(Cryptomeria Ciphering)が使用される。

【００３３】

ＤＶＤメディア１には、暗号化タイトルキー１４およびＣＣＩ(Copy Control Information)１５が記録される。暗号化タイトルキー１４は、暗号化されたタイトルキー情報であり、タイトルキー情報は、タイトル毎に付加される鍵情報である。ＣＣＩは、コピーノーモア、コピーワンス、コピーフリー等のコピー制御情報である。

【００３４】

レコーダ２は、デバイスキー２１、プロセスＭＫＢ２２、Ｃ２＿Ｇ２３、乱数発生器２４、Ｃ２＿Ｅ２５、Ｃ２＿Ｇ２６およびＣ２＿ＥＣＢＣ２７の構成要素を有する。プレーヤ３は、デバイスキー３１、プロセスＭＫＢ３２、Ｃ２＿Ｇ３３、Ｃ２＿Ｄ３５、Ｃ２＿Ｇ３６およびＣ２＿ＤＣＢＣ３７の構成要素を有する

。

【００３５】

デバイスキー２１、３１は、個々の装置メーカ、またはアプリケーションソフトウェアベンダー毎に発行された識別番号である。デバイスキーは、ライセンス管理者によって正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の情報である。ＤＶＤメディア１から再生されたＭＫＢ１２とデバイスキー２１とがプロセスＭＫＢ２２において演算されることによって、リボケーションされたかどうかの判別ができる。レコーダ２におけるのと同様に、プレーヤ３においても、ＭＫＢ１２とデバイスキー３１とがプロセスＭＫＢ３２において演算され、リボケーションされたかどうかの判別がなされる。

【００３６】

さらに、プロセスＭＫＢ２２、３２のそれぞれにおいて、ＭＫＢ１２とデバイスキー２１、３１からメディアキーが算出される。ＭＫＢ１２の中にレコーダ２またはプレーヤ３のデバイスキーが入っておらず、演算された結果が予め決められたある値例えばゼロの値と一致した場合、そのデバイスキーを持つレコーダ２またはプレーヤ３が正当なものでないと判断される。すなわち、そのようなレコーダ２またはプレーヤ３がリボケーションされる。

【００３７】

Ｃ２＿Ｇ２３、３３は、それぞれ、メディアキーとメディアＩＤとを演算し、メディアユニークキーを導出する処理である。

【００３８】

乱数発生器（ＲＮＧ：Random Number Generator）２４は、タイトルキーの生成に利用される。乱数発生器２４からのタイトルキーがＣ２＿Ｅ２５に入力され、タイトルキーがメディアユニークキーで暗号化される。暗号化タイトルキー１４がＤＶＤメディア１に記録される。

【００３９】

プレーヤ３では、ＤＶＤメディア１から再生された暗号化タイトルキー１４とメディアユニークキーとがＣ２＿Ｄ３５に供給され、暗号化タイトルキーがメデ

ィアユニークキーで復号され、タイトルキーが得られる。

【００４０】

レコーダ２においては、ＣＣＩとタイトルキーとがＣ２＿Ｇ２６に供給され、コンテンツキーが導出される。コンテンツキーがＣ２＿ＥＣＢＣ２７に供給され、コンテンツキーを鍵としてコンテンツが暗号化される。暗号化コンテンツ１３がＤＶＤメディア１に記録される。

【００４１】

プレーヤ３においては、ＣＣＩとタイトルキーとがＣ２　Ｇ３６に供給され、コンテンツキーが導出される。コンテンツキーがＣ２　ＥＣＢＣ３７に供給され、ＤＶＤメディア１から再生された暗号化コンテンツ１３がコンテンツキーを鍵として復号される。

【００４２】

図１の構成において、レコーダ２による記録の手順について説明する。レコーダ２は、ＤＶＤメディア１からＭＫＢ１２を読み出し、プロセスＭＫＢ２２によってデバイスキー２１とＭＫＢ１２とを演算し、メディアキーを計算する。演算結果が予め定められた値を示すならば、デバイスキー２１（レコーダ２の機器またはアプリケーション）がＭＫＢによってリボークされたと判定され、レコーダ２は、以後の処理を中断し、ＤＶＤメディア１への記録を禁止する。若し、メディアキーの値が予め定められた値以外であれば、処理を継続する。

【００４３】

次に、レコーダ２は、ＤＶＤメディア１からメディアＩＤ１１を読み、メディアキーと共にメディアＩＤをＣ２＿Ｇ２３に入力しメディア毎に異なるメディアユニークキーが演算される。乱数発生器２４で発生させたタイトルキーがＣ２＿Ｅ２５で暗号化され、暗号化タイトルキー１４としてＤＶＤメディア１に記録される。また、タイトルキーとコンテンツのＣＣＩ情報がＣ２＿Ｇ２６で演算され、コンテンツキーが導出される。コンテンツキーでコンテンツをＣ２＿ＥＣＢＣ２７で暗号化し、ＤＶＤメディア１上に暗号化コンテンツ１３としてＣＣＩ１５と共に記録する。

【００４４】

プレーヤ３による再生の手順について説明する。最初にＭＫＢ１２をＤＶＤメディア１から読み出し、デバイスキー３１とＭＫＢ１２を演算し、リボケーションの確認がなされる。デバイスキー３１、すなわち、プレーヤ３の機器またはアプリケーションがリボークされない場合には、メディアＩＤを使用してメディアユニークキーが演算され、読み出された暗号化タイトルキー１４とメディアユニークキーからタイトルキーが演算される。タイトルキーとＣＣＩ１５とがＣ２＿Ｇ３６に入力され、コンテンツキーが導出される。コンテンツキーがＣ２＿ＤＣＢＣ３７に入力され、コンテンツキーを鍵として、ＤＶＤメディア１から再生された暗号化コンテンツ１３に対してＣ２＿ＤＣＢＣ３７の演算が施される。その結果、暗号化コンテンツ１３が復号される。

【００４５】

このように、コンテンツの復号に必要なコンテンツキーを得るためには、ＤＶＤメディアの１枚毎に異なるメディアＩＤが必要となるので、たとえメディア上の暗号化コンテンツが忠実に他のメディアにコピーされても、他のメディアのメディアＩＤがオリジナルのメディアＩＤと異なるために、コピーされたコンテンツを復号することができず、コンテンツの著作権を保護することができる。

【００４６】

上述した図１の構成は、記録再生機器として構成されたものである。この発明は、ＤＶＤメディア１に対するコンテンツ保護処理をＰＣ環境下で扱う場合に適用される。図２を参照して現行の方式によるＰＣとドライブの役割分担を示す。図２において、参照符号４が上述したＣＰＲＭ規格に準拠したＤＶＤメディア１を記録および再生する記録再生装置としてのＤＶＤドライブを示す。

【００４７】

参照符号５がデータ処理装置としてのホスト例えばＰＣを示す。ホスト５は、ＤＶＤメディア１に記録可能で、ＤＶＤメディア１から再生可能なコンテンツを扱うことができ、且つＤＶＤドライブ４と接続されてデータ交換が可能な装置またはアプリケーションソフトウェアである。例えばＰＣに対してアプリケーションソフトウェアがインストールされることによってホスト５が構成される。

【００４８】

ＤＶＤドライブ４とホスト５との間がインターフェース４ａで接続されている。インターフェース４ａは、ＡＴＡＰＩ(AT Attachment with Packet Interface)，ＳＣＳＩ(Small Computer System Interface)，ＵＳＢ(Universal Serial Bus)，ＩＥＥＥ(Institute of Electrical and Electronics Engineers)１３９４等である。

【００４９】

ＤＶＤメディア１には、メディアＩＤ１１、メディアキーブロック１２およびＡＣＣ(Authentication Control Code)が予め記録されている。ＡＣＣは、ＤＶＤドライブ４とホスト５との間の認証がＤＶＤメディア１によって異なるようにするために予めＤＶＤメディア１に記録されたデータである。

【００５０】

ＤＶＤドライブ４は、ＡＣＣ１６をＤＶＤメディア１から読み出す。ＤＶＤメディア１から読み出されたＡＣＣ１６がＤＶＤドライブ４のＡＫＥ(Authentication and Key Exchange)４１に入力されると共に、ホスト５へ転送される。ホスト５は、受け取ったＡＣＣをＡＫＥ５１に入力する。ＡＫＥ４１および５１は、乱数データを交換し、この交換した乱数とＡＣＣの値とから認証動作の度に異なる値となる共通のセッションキー（バスキーと称する）を生成する。

【００５１】

バスキーがＭＡＣ(Message Authentication Code)演算ブロック４２および５２にそれぞれ供給される。ＭＡＣ演算ブロック４２および５２は、ＡＫＥ４１および５１でそれぞれ得られたバスキーをパラメータとして、メディアＩＤおよびメディアキーブロック１２のＭＡＣを計算するプロセスである。ＭＫＢとメディアＩＤの完全性(integrity)をホスト５が確認するために利用される。

【００５２】

ＭＡＣ４２および５２によってそれぞれ計算されたＭＡＣがホスト５の比較５３において比較され、両者の値が一致するかどうかが判定される。これらのＭＡＣの値が一致すれば、ＭＫＢとメディアＩＤの完全性が確認されたことになる。比較出力でスイッチＳＷ１が制御される。

【００５３】

スイッチＳＷ１は、ＤＶＤドライブ４のＤＶＤメディア１の記録または再生経路と、ホスト５の暗号化／（または）復号モジュール５４との間の信号路をＯＮ／ＯＦＦするものとして示されている。なお、スイッチＳＷ１は、信号路のＯＮ／ＯＦＦを行うものとして示されているが、より実際には、ＯＮの場合にホスト５の処理が継続し、ＯＦＦの場合にホスト５の処理が停止することを表している。暗号化／復号モジュール５４は、メディアユニークキーと暗号化タイトルキーとＣＣＩとからコンテンツキーを算出し、コンテンツキーを鍵としてコンテンツを暗号化コンテンツ１３へ暗号化し、またはコンテンツキーを鍵として暗号化コンテンツ１３を復号する演算ブロックである。

【００５４】

メディアユニークキー演算ブロック５５は、ＭＫＢ１２とメディアＩＤとデバイスキー５６とからメディアユニークキーを演算する演算ブロックである。すなわち、図１に示すレコーダまたはプレーヤと同様に、デバイスキーとＭＫＢ１２とからメディアキーが演算され、さらに、メディアキーとメディアＩＤ１１とからメディアユニークキーが演算される。メディアキーが所定の値となった場合には、その電子機器またはアプリケーションソフトウェアが正当なものではないと判断され、リボークされる。したがって、メディアユニークキー演算ブロック５５は、リボケーションを行うリボーク処理部としての機能も有する。

【００５５】

記録時に、比較５３によって完全性が確認された場合には、スイッチＳＷ１がＯＮされ、暗号化／復号モジュール５４からスイッチＳＷ１を通じてドライブ４に対して、暗号化コンテンツ１３、暗号化タイトルキー１４およびＣＣＩ１５が供給され、ＤＶＤメディア１に対してそれぞれ記録される。再生時に、比較５３によって完全性が確認された場合には、スイッチＳＷ１がＯＮされ、ＤＶＤメディア１からそれぞれ再生された暗号化コンテンツ１３、暗号化タイトルキー１４およびＣＣＩ１５がスイッチＳＷ１を通じてホスト５の暗号化／復号モジュール５４に対して供給され、暗号化コンテンツが復号される。

【００５６】

図３は、図２に示す現行のＰＣ環境下のＤＶＤメディアを利用するシステムに

おいて、ＤＶＤメディア１と、ＤＶＤドライブ４と、ホスト５との間の信号の授受の手順を示す。ホスト５がＤＶＤドライブ４に対してコマンドを送り、ＤＶＤドライブ４がコマンドに応答した動作を行う。

【００５７】

最初に、ホスト５からの要求に応じてＤＶＤメディア１上のＡＣＣがシークされ、読み出される（ステップＳ１）。次のステップＳ２において、読み出されたＡＣＣがＡＫＥ４１に入力されると共に、ホスト５へ転送され、ホスト５では、受け取ったＡＣＣがＡＫＥ５１へ入力される。ＡＫＥ４１および５１は、乱数データを交換し、この交換した乱数とＡＣＣ１６の値から認証動作の度に異なる値となるセッションキーとしてのバスキーを生成し、バスキーをＤＶＤドライブ４とホスト５が共有する。相互認証が成立しなかった場合では、処理が中断する。

【００５８】

認証動作は、電源のＯＮ後のディスク検出時並びにディスクの交換時には、必ず行われる。また、記録ボタンを押して記録動作を行う場合、並びに再生ボタンを押して再生動作を行う場合に、認証動作を行うようにしても良い。一例として、記録ボタンまたは再生ボタンを押した時に、認証がなされる。

【００５９】

認証が成功すると、次に、ステップＳ３において、ホスト５がＤＶＤドライブ４に対して、ＤＶＤメディア１からのＭＫＢ（メディアキーブロック）パック＃０の読み出しを要求する。ＭＫＢは、パック０～パック１５の１６セクタが１２回繰り返してリードインエリアに記録されている。パック単位で、エラー訂正符号化がなされている。

【００６０】

ＤＶＤドライブ４がステップＳ４においてＭＫＢのパック＃０を読みに行き、ステップＳ５において、パック＃０が読み出される。ＤＶＤドライブ４は、モディフアイドＭＫＢをホスト５へ戻す（ステップＳ６）。すなわち、ＭＫＢを読み出す際に、バスキーをパラメータとしてＭＡＣ値を計算し、ＭＫＢに対してＭＡＣ値を付加してホスト５へデータを転送する。パック＃０以外の残りのＭＫＢパックの要求と、ＤＶＤドライブ４の読み出し動作と、モディフアイドＭＫＢパッ

クの転送動作とがＭＫＢのパックがなくなるまで、例えばパック＃１５が読み出され、ホスト５へ転送されるまで、ステップＳ７およびＳ８によって繰り返しなされる。

【００６１】

次に、ホスト５がＤＶＤドライブ４に対してメディアＩＤを要求する。ＤＶＤドライブ４がＤＶＤメディア１に記録されているメディアＩＤを読みに行き、ステップＳ１１において、メディアＩＤが読み出される。ＤＶＤドライブ４は、メディアＩＤを読み出す際に、バスキーをパラメータとしてそのＭＡＣ値を計算し、ステップＳ１２において、読み出されたメディアＩＤに対してＭＡＣ値ｍ１を付加してホスト５へデータを転送する。

【００６２】

ホスト５では、ＤＶＤドライブ４から受け取ったＭＫＢ１２およびメディアＩＤ１１からバスキーをパラメータとして再度ＭＡＣ値を計算し、計算したＭＡＣ値とＤＶＤドライブ４から受け取ったＭＡＣ値とを比較５３で比較し、両者が一致したならば、正しいＭＫＢおよびメディアＩＤを受け取ったと判定して、スイッチＳＷ１をＯＮに設定して処理を先に進める。逆に両者が一致しなかったならば、ＭＫＢおよびメディアＩＤが改ざんされたものと判定して、スイッチＳＷ１をＯＦＦに設定して処理を中断する。

【００６３】

ステップＳ１３において、ホスト５がＤＶＤドライブ４に対して暗号化コンテンツを要求し、ステップＳ１４において、ＤＶＤドライブ４が暗号化コンテンツを読み出し、ステップＳ１３において、読み出した暗号化コンテンツがホスト５に転送される。ホスト５のメディアユニークキー演算ブロック５５では、デバイスキー５６とＭＫＢ１２とメディアＩＤ１１とによってメディアユニークキーが計算される。そして、メディアユニークキーが暗号化／復号モジュール５４に供給され、暗号化タイトルキー１４、ＣＣＩ１５からコンテンツキーが求められ、コンテンツキーを鍵としてＤＶＤメディア１から読み出された暗号化コンテンツが復号され、また、ＤＶＤメディア１に対して記録されるコンテンツが暗号化される。

【００６４】

図４のフローチャートにおいて、ステップＳＴ１は、ＭＡＣ演算ブロック４２でバスキーをパラメータとして求められたＭＡＣ計算値と、ＭＡＣ演算ブロック５３でバスキーをパラメータとして求められたＭＡＣ計算値とを比較するステップである。両者が一致すれば、スイッチＳＷ１がステップＳＴ２においてＯＮとされ、両者が一致しない場合では、スイッチＳＷ１がステップＳＴ３においてＯＦＦとされ、処理が停止する。

【００６５】

上述したＣＰＲＭでは、ＤＶＤ－Videoの著作権保護技術であるＣＳＳと同じバスキー生成方法を採用している。ＣＳＳ認証方式の内容は、本来秘密であるべき情報であるが、既に解析され一般ユーザーが入手可能なＣＳＳライセンス管理団体であるDVD-CCAの許諾を得ていないフリーソフトウェアによって動作させることが可能となっている。また、コンテンツプロテクション処理は、ホスト側でなされる、すなわち、リボケーション判定、メディアキー取得、メディアユニークキー導出、タイトルキー生成・導出からコンテンツキー導出およびコンテンツ暗号化・復号の全てがホスト側の処理であることから、著作権保護技術としての信頼性が低下している。

【００６６】

以下に述べるこの発明は、かかる問題点を解決するものである。一実施形態では、ＰＣ環境下でのコンテンツプロテクション処理におけるＰＣとドライブの役割分担におけるリボケーション動作とメディアキー導出に関わる情報（ここでは、デバイスキー）をドライブ内部に持ち、ＰＣとの相互認証を経てセッションキーを導出するものである。

【００６７】

図５は、一実施形態における相互認証の構成を示すブロック図であり、図６は、ドライブ側の処理の流れを示すフローチャートであり、図７は、ホスト側の処理の流れを示すフローチャートである。以下の説明において、参照符号１０１がメディア例えば光ディスクを示し、参照符号１０２がメディアのドライブを示し、参照符号１０３がドライブ１０２とドライブ－ホストインターフェース１０４

を介して接続されたホストを示す。メディア１０１は、上述したＤＶＤメディアと同様の情報が予め記録されているものである。メディア１０１は、記録可能なものに限らず、読み出し専用のものでも良い。ホスト１０３がドライブ１０２に対して所定のコマンドを送り、その動作を制御する。使用するコマンドは、上述した非特許文献２に記載されているコマンド並びにコマンドを拡張したもの、および、メディア１０１からコンテンツをセクタ・データとして読み出すためのＲＥＡＤコマンド、メディア１０１へコンテンツをセクタ・データとして書き込むためのＷＲＩＴＥコマンドである。

【００６８】

ドライブ１０２は、ドライブのデバイスキー１２１を有し、ホスト１０３がホストのデバイスキー１３１を有している。デバイスキー１２１は、多くの場合にＬＳＩ(Large Scale Integrated Circuit：大規模集積回路)内部に配置され、外部から読み出すことができないようセキュアに記憶される。デバイスキー１３１は、ソフトウェアプログラム内にセキュアに記憶される場合と、ハードウェアとしてセキュアに記憶される場合とがある。また、ドライブ１０２がメディア１０１を扱う正当なドライブとなるためには、一実施形態のように、デバイスキーのような著作権保護技術に関する秘密情報を必要とするので、正規のライセンスを受けずに正規品になりすますようなクローン・ドライブの作成を防止できる効果がある。

【００６９】

図５に示すように、ドライブ１０２には、ＭＫＢとデバイスキー１２１とが入力され、ドライブのデバイスキーがリボケーションされたかどうかを判定するプロセスＭＫＢ１２２が備えられている。ホスト１０３にも同様に、プロセスＭＫＢ１３２が備えられている。リボケーションされない場合に、プロセスＭＫＢ１２２および１３２からそれぞれメディアキーＫｍが出力される。リボーク判定処理がなされ、メディアキーＫｍが得られてから認証処理がなされる。

【００７０】

参照符号１２３、１２４および１２５は、メディアキーＫｍをパラメータとしてＭＡＣ値を計算するＭＡＣ演算ブロックをそれぞれ示す。また、参照符号１２

６、１２７および１２８は、乱数発生器（ＲＮＧ：Random Number Generator)をそれぞれ示す。乱数発生器１２６が乱数Ｒalを生成し、乱数発生器１２７が乱数Ｒa2を生成し、乱数発生器１２８が乱数Ｒa3を生成する。乱数発生器１２６、１２７、１２８は、例えばＬＳＩの構成の乱数発生器であり、ソフトウェアにより乱数を発生する方法と比較してより真正乱数に近い乱数を発生することができる。乱数発生器を共通のハードウエアとしても良いが、乱数Ｒal、Ｒa2、Ｒa3は、互いに独立したものである。

【００７１】

ホスト１０３に、メディアキーＫｍをパラメータとしてＭＡＣ値を計算するＭＡＣ演算ブロック１３３、１３４および１３５と、乱数発生器１３６、１３７および１３８が備えられている。乱数発生器１３６が乱数Ｒblを生成し、乱数発生器１３７が乱数Ｒb2を生成し、乱数発生器１３８が乱数Ｒb3を生成する。乱数発生器１３６、１３７、１３８は、通常はソフトウェアによって乱数を発生するものであるが、ハードウェアによる乱数が利用できる場合にはこれを用いても良い。

【００７２】

ドライブ１０２において生成された乱数とホスト１０３において生成された乱数とが交換される。すなわち、乱数Ｒalおよび乱数ＲblがＭＡＣ演算ブロック１２３および１３３に入力され、乱数Ｒa2および乱数Ｒb2がＭＡＣ演算ブロック１２４および１３４に入力され、乱数Ｒa3および乱数Ｒb3がＭＡＣ演算ブロック１２５および１３５に入力される。

【００７３】

ドライブ１０２のＭＡＣ演算ブロック１２３が演算したＭＡＣ値と、ホスト１０３のＭＡＣ演算ブロック１３３が演算したＭＡＣ値とがホスト１０３内の比較１３９において比較され、二つの値が同一か否かが判定される。ここでのＭＡＣ値は、eKm(Ral‖Rbl)と表記される。ｅＫｍ（）は、メディアキーＫｍを鍵として括弧内のデータを暗号化することを表している。Ｒal‖Ｒblの記号は、左側に乱数Ｒalを配し、右側に乱数Ｒblを配するように、二つの乱数を結合することを表している。比較の結果、二つの値が同一と判定されると、ホスト１０３による

ドライブ１０２の認証が成功したことになり、そうでない場合には、この認証が失敗したことになる。

【００７４】

ホスト１０３のＭＡＣ演算ブロック１３４が演算したＭＡＣ値と、ドライブ１０２のＭＡＣ演算ブロック１２４が演算したＭＡＣ値とがドライブ１０２内の比較１２９において比較され、二つの値が同一か否かが判定される。ここでのＭＡＣ値は、eKm(Rb2‖Ra2)と表記される。比較の結果、二つの値が同一と判定されると、ドライブ１０２によるホスト１０３の認証が成功したことになり、そうでない場合には、この認証が失敗したことになる。

【００７５】

かかる相互認証において、比較１３９および１２９の両者において、ＭＡＣ値が同一と判定され、ドライブ１０２およびホスト１０３の両者の正当性が確認されると、すなわち、相互認証が成功すると、ＭＡＣ演算ブロック１２５および１３５によって、共通のセッションキーeKm(Ra3‖Rb3)がそれぞれ生成される。

【００７６】

さらに、上述した相互認証の処理の流れを図６および図７のフローチャートを参照して説明する。最初に、図７のステップＳＴ２０において、ホスト１０３がドライブ１０２に対して、コマンドREPORT KEYを発行し、ＭＫＢの転送を要求する。図６のステップＳＴ１０において、ドライブ１０２がメディア１０１からＭＫＢ１１２を読み出して、ホスト１０３へ転送する。

【００７７】

次に、ドライブ１０２がステップＳＴ１１において、プロセスＭＫＢ１２２によってメディアキーＫｍを計算し、ホスト１０３がステップＳＴ２１において、プロセスＭＫＢ１３２によってメディアキーＫｍを計算する。この計算の過程でそれぞれが内蔵するデバイスキー１２１および１３１がリボケーションの対象とされているか否かが自分自身によって確認される（図６中のステップＳＴ１２、図７中のステップＳＴ２２）。

【００７８】

ドライブ１０２およびホスト１０３のそれぞれは、リボケーションの対象とさ

れている場合にはリボークされ、処理が終了する。若し、ホスト１０３がリボケーションの対象とされていなければ、ステップＳＴ２３において、コマンドSEND KEYにより、ドライブ１０２に対して乱数発生器１３６および１３７でそれぞれ生成された乱数Rb1と乱数Rb2を転送する。若し、ドライブ１０２がリボケーションの対象とされていなければ、ステップＳＴ１３において、ドライブ１０２がホスト１０３から転送されたこれらの乱数を受け取る。

【００７９】

その後、ホスト１０３は、コマンドREPORT KEYによりドライブ１０２に対してドライブ１０２が持つメディアキーＫｍを鍵としたＭＡＣによるレスポンス値と乱数生成器１２６が発生した乱数Raltをホスト１０３へ転送することを要求する（ステップＳＴ２４）。このレスポンス値は、eKm(Ral‖Rb1)と表記される。ｅＫｍ（）は、メディアキーＫｍを暗号鍵として括弧内のデータを暗号化することを表している。Ral‖Rb1の記号は、左側に乱数Ralを配し、右側に乱数Rb1を配するように、二つの乱数を結合することを表している。

【００８０】

ホスト１０３からコマンドREPORT KEYを受け取ったドライブ１０２は、ステップＳＴ１４において、ＭＡＣ演算ブロック１２３が生成したＭＡＣ値eKm(Ral‖Rb1)と乱数Ralをホスト１０３へ転送する。ステップＳＴ２５において、ホスト１０３は、自身のＭＡＣ演算ブロック１３３でＭＡＣ値を計算し、比較１３９においてドライブ１０２から受け取った値と一致するかの確認を行う。若し、受け取ったＭＡＣ値と計算されたＭＡＣ値とが一致したのなら、ホスト１０３によるドライブ１０２の認証が成功したことになる。ステップＳＴ２５における比較の結果が同一でない場合には、ホスト１０３によるドライブ１０２の認証が失敗したことになり、リジェクト処理がなされる。

【００８１】

ホスト１０３によるドライブ１０２の認証が成功した場合には、ステップＳＴ２６において、ホスト１０３がドライブ１０２へコマンドREPORT KEYを送付し、ドライブ１０２の乱数生成器１２４および１２５がそれぞれ生成する乱数Ra2と乱数Ra3の転送を要求する。このコマンドに応答して、ステップＳＴ１５におい

て、ドライブ１０２は、これらの乱数をホスト１０３へ転送する。

【００８２】

ステップＳＴ２７において、ホスト１０３のＭＡＣ演算ブロック１３４は、ドライブ１０２から受け取った乱数からホスト１０３が持つメディアキーＫｍを鍵としたＭＡＣによるレスポンス値eKm(Rb2‖Ra2)を計算し、乱数Ｒb3とともに、コマンドSEND KEYを用いてドライブ１０２へ転送する。

【００８３】

ステップＳＴ１６において、ドライブ１０２は、ホスト１０３からレスポンス値eKm(Rb2‖Ra2)および乱数Rb3を受け取ると、自身でＭＡＣ値を計算し、ステップＳＴ１７において、比較１２９によってホスト１０３から受け取ったＭＡＣ値と一致するかの確認を行う。若し、受け取ったＭＡＣ値と計算されたＭＡＣ値とが一致したのなら、ドライブ１０２によるホスト１０３の認証が成功したことになる。この場合には、ステップＳＴ１８において、ＭＡＣ演算ブロック１２５がセッションキーeKm(Ra3‖Rb3)を生成し、また、ホスト１０３に対して認証が成功したことを示す情報を送信し、認証処理が完了する。セッションキーは、認証動作の度に異なる値となる。

【００８４】

ステップＳＴ１７における比較の結果が同一でない場合には、ドライブ１０２によるホスト１０３の認証が失敗したことになり、ステップＳＴ１９において、認証が失敗したことを示すエラー情報がホスト１０３に送信される。

【００８５】

ホスト１０３は、送付したコマンドSEND KEYに対する応答としてドライブ１０２から認証が成功したか否かを示す情報を受け取り、受け取った情報に基づいてステップＳＴ２８において、認証完了か否かを判断する。認証が成功したことを示す情報を受け取ることで認証完了と判断し、認証が失敗したことを示す情報を受け取ることで認証が完了しなかったと判断する。認証が完了した場合は、ステップＳＴ２９において、ＭＡＣ演算ブロック１３５がドライブ側と共通のセッションキーeKm(Ra3‖Rb3)（例えば６４ビット長）を生成する。認証が完了しなかった場合には、リジェクト処理がなされる。セッションキーeKm(Ra3‖Rb3)を以

下の説明では、適宜Ｋｓと表記する。

【００８６】

上述した一実施形態による相互認証は、ドライブ１０２がリボケーション機能を持つことができ、また、認証専用の特定の認証鍵を必要としない特徴を有している。

【００８７】

また、電子機器固有の情報としてのデバイスキーを記録再生装置が持つことによって、記録再生装置自身をリボークすることが可能となる。

【００８８】

さらに、ドライブ１０２が比較１２９によってホスト１０３の認証結果を確認することで、ドライブ１０２がホスト１０３から正規のライセンスを受けた上で実装されたものであるか否かを判定することが可能となる。

【００８９】

次に、上述した相互認証を行うドライブ１０２とホスト１０３とを組み合わせて実現したレコーダの一実施形態の構成を図８に示す。一実施形態のレコーダは、ドライブ１０２がメディアユニークキーを計算し、計算したメディアユニークキーを相互認証によって生成したセッションキーＫｓを用いてセキュアにホスト１０３に転送する。また、ドライブ１０２がコンテンツキー導出のための乱数データを生成し、生成した乱数データを相互認証によって生成したセッションキーＫｓを用いてホスト１０３へセキュアに転送し、ホスト１０３が導出したコンテンツキーを用いてコンテンツを暗号化し、暗号化コンテンツをドライブ１０２へ転送し、ドライブ１０２が暗号化コンテンツをメディア１０１へ記録する構成とされている。

【００９０】

レコーダを構成するドライブ１０２は、デバイスキー１２１、プロセスＭＫＢ１２２、Ｃ２＿Ｇ２１４１、ＤＥＳ(Data Encryption Standard)エンクリプタ１４２、乱数発生器１４３、ＤＥＳエンクリプタ１４４の構成要素を有する。

【００９１】

メディア１０１から再生されたＭＫＢ１１２とデバイスキー１２１とがプロセ

スＭＫＢ１２２において演算されることによって、リボケーションされたかどうかの判別ができる。プロセスＭＫＢ１２２において、ＭＫＢ１１２とデバイスキー１２１からメディアキーが算出される。ＭＫＢ１１２の中にドライブ１０２のデバイスキー１２１が入っておらず、演算された結果が予め決められたある値例えばゼロの値と一致した場合、そのデバイスキー１２１を持つドライブ１０２が正当なものでないと判断され、ドライブ１０２がリボケーションされる。

【００９２】

Ｃ２＿Ｇ１４１は、メディアキーとメディアＩＤ１１１とを演算し、メディアユニークキーを導出する処理である。メディアユニークキーがＤＥＳエンクリプタ１４２にてセッションキーＫｓによって暗号化される。暗号化の方式として、例えばＤＥＳ　ＣＢＣモードが使用される。ＤＥＳエンクリプタ１４２の出力がホスト１０３のＤＥＳデクリプタ１５１に送信される。

【００９３】

乱数発生器１４３によってタイトルキーが生成される。乱数発生器１４３からのタイトルキーがＤＥＳエンクリプタ１４４に入力され、タイトルキーがセッションキーで暗号化される。暗号化タイトルキーがホスト１０３のＤＥＳデクリプタ１５２に送信される。

【００９４】

ホスト１０３において、ＤＥＳデクリプタ１５１において、セッションキーＫｓによってメディアユニークキーが復号される。ＤＥＳデクリプタ１５２において、セッションキーＫｓによってタイトルキーが復号される。メディアユニークキーおよびタイトルキーがＣ２＿Ｅ１５３に供給され、タイトルキーがメディアユニークキーを使用してＣ２によって暗号化される。暗号化タイトルキー１１４がメディア１０１に記録される。

【００９５】

ホスト１０３においては、ＣＣＩと復号されたタイトルキーとがＣ２＿Ｇ１５４に供給され、コンテンツキーが導出される。コンテンツキーがＣ２＿ＥＣＢＣ１５５に供給され、コンテンツキーを鍵としてコンテンツが暗号化される。暗号化コンテンツ１１３がメディア１０１に記録される。

【００９６】

図９は、コンテンツ記録時の手順を示すものである。最初に、ホスト１０３からの要求に応じてメディア１０１上のＭＫＢがシークされ、読み出される（ステップＳ２１）。次のステップＳ２２のＡＫＥ(Authentication and Key Exchange)において、上述したようなリボーク処理とドライブ１０２とホスト１０３の相互認証動作がなされる。

【００９７】

相互認証動作は、電源のＯＮ後のディスク検出時並びにディスクの交換時には、必ず行われる。また、記録ボタンを押して記録動作を行う場合、並びに再生ボタンを押して再生動作を行う場合に、認証動作を行うようにしても良い。一例として、記録ボタンまたは再生ボタンを押した時に、認証がなされる。

【００９８】

相互認証が成功しないと、リジェクト処理によって例えば処理が中断する。相互認証が成功すると、ドライブ１０２およびホスト１０３の両者において、セッションキーＫｓが生成され、セッションキーＫｓが共有される。

【００９９】

次のステップＳ２３において、ホスト１０３がドライブ１０２に対してメディアユニークキーを要求する。ドライブ１０２は、メディア１０１のメディアＩＤをシークし（ステップＳ２４）、メディアＩＤをメディア１０１から読み出す（ステップＳ２５）。ドライブ１０２は、メディアキーとメディアＩＤとを演算することによってメディアユニークキーを生成する。ステップＳ２６において、メディアユニークキーがセッションキーＫｓによって暗号化され、暗号化されたメディアユニークキーがホスト１０３に転送される。

【０１００】

次に、ステップＳ２７において、ホスト１０３がドライブ１０２に対してタイトルキーを要求する。ステップＳ２８において、ドライブ１０２がタイトルキーをセッションキーＫｓで暗号化し、暗号化したタイトルキーをホスト１０３に転送する。ホスト１０３において、セッションキーＫｓによって、暗号化されたメディアユニークキーおよび暗号化されたタイトルキーがそれぞれ復号される。

【０１０１】

そして、タイトルキーがメディアユニークキーによって暗号化され、暗号化タイトルキーが生成される。また、タイトルキーとＣＣＩからコンテンツキーが生成され、コンテンツキーによってコンテンツが暗号化される。ステップＳ２９において、ホスト１０３からドライブ１０２に対して、暗号化タイトルキー、暗号化コンテンツおよびＣＣＩが転送される。ステップＳ３０において、ドライブ１０２によって、これらの暗号化タイトルキー、暗号化コンテンツおよびＣＣＩがメディア１０１に対して記録される。

【０１０２】

なお、図８のレコーダの構成においては、ドライブ１０２において乱数発生器１４３を使用してタイトルキーを生成している。しかしながら、ホスト１０３に乱数発生器を設け、この乱数発生器によってタイトルキーを生成するようにしても良い。

【０１０３】

次に、上述した相互認証を行うドライブ１０２とホスト１０３とを組み合わせて実現したプレーヤの一実施形態の構成を図１０に示す。一実施形態のプレーヤは、ドライブ１０２が計算したメディアユニークキーを相互認証によって生成したセッションキーＫｓを用いてセキュアにホスト１０３に転送し、ホスト１０３が暗号化タイトルキーをメディアユニークキーによって復号し、タイトルキーとＣＣＩとから導出したコンテンツキーを用いてコンテンツを復号する構成とされている。

【０１０４】

プレーヤを構成するドライブ１０２は、デバイスキー１２１、プロセスＭＫＢ１２２、Ｃ２＿Ｇ２１４１、ＤＥＳエンクリプタ１４２の構成要素を有する。メディア１０１から再生されたＭＫＢ１１２とデバイスキー１２１とがプロセスＭＫＢ１２２において演算されることによって、リボケーションされたかどうかの判別ができる。プロセスＭＫＢ１２２において、ＭＫＢ１１２とデバイスキー１２１からメディアキーが算出される。

【０１０５】

Ｃ２＿Ｇ１４１は、メディアキーとメディアＩＤ１１１とを演算し、メディアユニークキーを導出する処理である。メディアユニークキーがＤＥＳエンクリプタ１４２にてセッションキーＫｓによって暗号化される。暗号化の方式として、例えばＤＥＳ　ＣＢＣモードが使用される。ＤＥＳエンクリプタ１４２の出力がホスト１０３のＤＥＳデクリプタ１５１に送信される。

【０１０６】

ホスト１０３において、ＤＥＳデクリプタ１５１において、セッションキーＫｓによってメディアユニークキーが復号される。メディアユニークキーおよび暗号化タイトルキー１１４がＣ２＿Ｄ１５３に供給され、暗号化タイトルキーがメディアユニークキーを使用して復号される。復号されたタイトルキーとメディア１０１から再生されたＣＣＩがＣ２＿Ｇ１５４に供給され、コンテンツキーが導出される。メディア１０１から再生された暗号化コンテンツ１１３がＣ２デクリプタ１５５において、コンテンツキーによって復号され、コンテンツが得られる。

【０１０７】

図１１は、コンテンツ再生時の手順を示すものである。最初に、ホスト１０３からの要求に応じてメディア１０１上のＭＫＢがシークされ、読み出される（ステップＳ４１）。ＭＫＢがパック毎に読み出される。次のステップＳ４２のＡＫＥにおいて、上述したようなリボーク処理とドライブ１０２とホスト１０３の相互認証動作がなされる。

【０１０８】

相互認証が成功しないと、リジェクト処理によって例えば処理が中断する。相互認証が成功すると、ドライブ１０２およびホスト１０３の両者において、セッションキーＫｓが生成され、セッションキーＫｓが共有される。

【０１０９】

次のステップＳ４３において、ホスト１０３がドライブ１０２に対してメディアユニークキーを要求する。ドライブ１０２は、メディア１０１のメディアＩＤをシークし（ステップＳ４４）、メディアＩＤをメディア１０１から読み出す（ステップＳ４５）。ドライブ１０２は、メディアキーとメディアＩＤとを演算す

ることによってメディアユニークキーを生成する。ステップＳ４６において、メディアユニークキーがセッションキーＫｓによって暗号化され、暗号化されたメディアユニークキーがホスト１０３に転送される。

【０１１０】

次に、ステップＳ４７において、ホスト１０３がドライブ１０２に対して、暗号化タイトルキー、ＣＣＩおよび暗号化コンテンツを要求する。ステップＳ４８において、ドライブ１０２が暗号化タイトルキー１１４、ＣＣＩ１１５および暗号化コンテンツ１１３をメディア１０１からリードする。ステップＳ４９において、ドライブ１０２が暗号化タイトルキー１１４、ＣＣＩ１１５および暗号化コンテンツ１１３を読み取る。そして、ステップＳ５０において、ドライブ１０２が暗号化タイトルキー１１４、ＣＣＩ１１５および暗号化コンテンツ１１３をホスト１０３に対して転送する。

【０１１１】

ホスト１０３において、タイトルキーが復号され、タイトルキーとＣＣＩとからコンテンツキーが求められ、コンテンツキーを鍵として暗号化コンテンツが復号される。

【０１１２】

図１０に示すプレーヤの構成においては、ホスト１０３が暗号化タイトルキーを復号するデクリプタＣ２＿Ｄ１５３を備えているが、ドライブ１０２が暗号化タイトルキーを復号するデクリプタを備えるようにしても良い。この場合、復号されたタイトルキーがホスト１０３のコンテンツキー生成用のＣ２＿Ｇ１５４に対してセキュアに転送される。または、ドライブ１０２にコンテンツキー生成装置Ｃ２＿Ｇを設け、ドライブ１０２において復号されたタイトルキーとＣＣＩとからコンテンツキーを生成するようにしても良い。この場合、復号されたコンテンツキーがホスト１０３のＣ２＿ＤＣＢＣ１５５へセキュアに転送される。

【０１１３】

図１２は、相互認証を行うドライブ１０２とホスト１０３とを組み合わせて実現したレコーダの他の実施形態の構成を示す。他の実施形態のレコーダは、ドライブ１０２が計算したメディアユニークキーを相互認証によって生成したセッシ

ョンキーＫｓを用いてセキュアにホスト１０３に転送する。また、ドライブ１０２においてコンテンツキーが生成され、生成されたコンテンツキーがセッションキーＫｓを用いてホスト１０３へセキュアに転送され、ホスト１０３が復号したコンテンツキーを用いてコンテンツを暗号化し、暗号化コンテンツをドライブ１０２へ転送し、ドライブ１０２が暗号化コンテンツをメディア１０１へ記録する構成とされている。すなわち、図８に示す上述したレコーダでは、ホスト１０３においてコンテンツキーを生成したが、他の実施形態では、ドライブ１０２において、コンテンツキーを生成している。

【０１１４】

図１２に示すように、メディア１０１から再生されたＭＫＢ１１２とデバイスキー１２１とがプロセスＭＫＢ１２２において演算されることによって、メディアキーが算出され、Ｃ２＿Ｇ１４１において、メディアキーとメディアＩＤ１１１とが演算し、メディアユニークキーが導出される。メディアユニークキーがＤＥＳエンクリプタ１４２にてセッションキーＫｓによって暗号化され、ＤＥＳエンクリプタ１４２の出力がホスト１０３のＤＥＳデクリプタ１５１に送信され、ＤＥＳデクリプタ１５１によってメディアユニークキーが導出される。

【０１１５】

さらに、ドライブ１０２の乱数発生器１４３によってタイトルキーが生成され、乱数発生器１４３からのタイトルキーがホスト１０３のＣ２＿Ｅ１５３に供給され、タイトルキーがメディアユニークキーを使用してＣ２によって暗号化される。暗号化タイトルキー１１４がメディア１０１に記録される。

【０１１６】

ホスト１０３において、セッションキーＫｓを鍵としてＭＡＣ演算ブロック１５８によりＣＣＩのＭＡＣ値ｅＫｓ（ＣＣＩ）が計算され、ＣＣＩとともにドライブ１０２へ転送される。

【０１１７】

ドライブ１０２において、ホスト１０３から受け取ったＣＣＩからセッションキーＫｓを鍵としてＭＡＣ演算ブロック１５７によりＣＣＩのＭＡＣ値ｅＫｓ（ＣＣＩ）が計算され、ホスト１０３から受け取ったＭＡＣ値とともに比較１５９

へ供給される。

【０１１８】

比較１５９では、両方のＭＡＣ値が一致したならば、ホスト１０３から受け取ったＣＣＩの改ざんは無いものと判断し、スイッチＳＷ２をＯＮする。一致しなかった場合は、ＣＣＩは改ざんされたものとみなし、スイッチＳＷ２をＯＦＦし、以降の処理を中断する。

【０１１９】

ドライブ１０２において、ホスト１０３から受け取ったＣＣＩとタイトルキーとがＣ２＿Ｇ１４５に供給され、コンテンツキーが導出される。コンテンツキーがＤＥＳエンクリプタ１４６に供給され、セッションキーＫｓを鍵として、コンテンツキーが暗号化される。暗号化コンテンツキーがホスト１０３のＤＥＳデクリプタ１５６に転送される。

【０１２０】

ＤＥＳデクリプタ１５６でセッションキーＫｓを鍵として復号されたコンテンツキーがＣ２＿ＥＣＢＣ１５５に供給され、コンテンツキーを鍵としてコンテンツが暗号化される。暗号化コンテンツ１１３がドライブ１０２に転送され、ドライブ１０２によってメディア１０１に記録される。

【０１２１】

なお、図１２に示すレコーダにおいては、タイトルキーがドライブ１０２の乱数発生器１４３によって生成されている。しかしながら、ホスト１０３側に乱数発生器を設け、この乱数発生器によってタイトルキーを生成しても良い。この場合には、生成されたタイトルキーがホスト１０３からドライブ１０２のコンテンツキー生成のためのＣ２＿Ｇ１４５に対して転送される。

【０１２２】

図１３は、レコーダの他の実施形態によるコンテンツ記録時の手順を示すものである。最初に、ホスト１０３からの要求に応じてメディア１０１上のＭＫＢがシークされ、読み出される（ステップＳ６１）。次のステップＳ６２のＡＫＥにおいて、リボーク処理とドライブ１０２とホスト１０３の相互認証動作がなされる。

【０１２３】

相互認証が成功しないと、リジェクト処理によって例えば処理が中断する。相互認証が成功すると、ドライブ１０２およびホスト１０３の両者において、セッションキーＫｓが生成され、セッションキーＫｓが共有される。

【０１２４】

次のステップＳ６３において、ホスト１０３がドライブ１０２に対してメディアユニークキーを要求する。ドライブ１０２は、メディア１０１のメディアＩＤをシークし（ステップＳ６４）、メディアＩＤをメディア１０１から読み出す（ステップＳ６５）。ドライブ１０２は、メディアキーとメディアＩＤとを演算することによってメディアユニークキーを生成する。ステップＳ６６において、メディアユニークキーがセッションキーＫｓによって暗号化され、暗号化されたメディアユニークキーがホスト１０３に転送される。

【０１２５】

次に、ステップＳ６７において、ホスト１０３がドライブ１０２に対してタイトルキーを要求する。ステップＳ６８において、ドライブ１０２がタイトルキーをホスト１０３に転送する。ホスト１０３において、セッションキーＫｓによって、暗号化されたメディアユニークキーが復号される。そして、タイトルキーがメディアユニークキーによって暗号化され、暗号化タイトルキーが生成される。

【０１２６】

また、ステップＳ６９において、ホスト１０３がドライブ１０２に対してＣＣＩを送る。このとき、ＣＣＩの改ざんを回避するためにＣＣＩの認証データとして計算されたＭＡＣ値ｅＫｓ（ＣＣＩ）を付加して転送する。ドライブ１０２において、ＣＣＩの改ざんが無いことを確認後、タイトルキーとＣＣＩからコンテンツキーが生成され、コンテンツキーがセッションキーＫｓで暗号化される。ステップＳ７０において、ホスト１０３がドライブ１０２に対してコンテンツキーを要求すると、ステップＳ７１において、ドライブ１０２が暗号化されたコンテンツキーをホスト１０３に送る。

【０１２７】

ホスト１０３は、暗号化コンテンツキーをセッションキーＫｓによって復号し

、コンテンツキーを得る。コンテンツキーによってコンテンツが暗号化される。ステップＳ７２において、ホスト１０３からドライブ１０２に対して、暗号化タイトルキー、暗号化コンテンツおよびＣＣＩが転送される。ステップＳ７３において、ドライブ１０２によって、暗号化タイトルキー、暗号化コンテンツおよびＣＣＩがメディア１０１に対して記録される。

【０１２８】

上述した図１２に示す構成のレコーダは、ドライブ１０２において、真正乱数またはそれに近い乱数をハードウエア例えばＬＳＩによって発生することができ、生成した乱数を固定値への置き換えを困難とすることができる。また、ドライブ１０２において、ハードウエア構成によってコンテンツキーを生成するので、著作権保護の実装を強力とすることができる。

【０１２９】

この発明は、上述したこの発明の一実施形態等に限定されるものではなく、この発明の要旨を逸脱しない範囲内で様々な変形や応用が可能である。例えばタイトルキーは、タイトル毎のキーであるが、この発明では、乱数情報であれば、タイトル毎に異なることは、必要ではない。

【０１３０】

また、上述した説明においては、著作権保護技術としてＣＰＲＭおよびＣＰＲＭを拡張した例を挙げたが、ＣＰＲＭ以外の著作権保護技術に対してもこの発明を適用することができる。例えば、特開2001－352322号公報において提案されるツリー構造の鍵配布構成に基づく著作権保護技術に対して適用可能である。また、ＰＣベースのシステムに対してこの発明が適用されるが、このことは、ＰＣとドライブを組み合わせる構成にのみ限定されることを意味するものではない。例えば携帯型動画または静止画カメラの場合に、メディアとして光ディスクを使用し、メディアを駆動するドライブとドライブを制御するマイクロコンピュータが設けられる動画または静止画カメラシステムに対してもこの発明を適用することが可能である。

【０１３１】

【発明の効果】

この発明では、メディア上に記録された鍵情報（ＭＫＢ）と各デバイスまたは各アプリケーションに記憶されている鍵情報（デバイスキー）から同一の値として導かれる鍵情報（メディアキー）を利用して相互認証がなされる。したがって、この発明においては、認証のためだけに用意される特定の認証鍵を必要とせず、秘密情報を少なくでき、また、デバイスまたはアプリケーションによってデバイスキーを異ならせることが可能であるので、秘密情報が不正に読み取られる危険性を少なくできる。

【０１３２】

この発明では、著作権保護技術に関する秘密情報である電子機器またはアプリケーションソフトウェア固有の情報例えばデバイスキーがドライブ内に実装されているので、情報処理装置にインストールされるアプリケーションソフトウェアは、著作権保護技術に関する秘密情報の全てを持つ必要がなくなる。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持たせることが容易に実施でき、また、ディスクからのデータとしてそのまま読み出された暗号化コンテンツが「ＤｅＣＳＳ」のような解読ソフトウェアにより復号され、平文のままのクリア・コンテンツとしてコピー制限の働かない状態で複製が繰り返されるような事態を防ぐことができることから、著作権保護技術の安全性を確保することができる。

【０１３３】

また、電子機器固有の情報としてのデバイスキーを記録再生装置が持つことによって、記録再生装置自身をリボークすることが可能となる。

【０１３４】

さらに、この発明では、情報処理装置におけるコンテンツキーを計算するのに必要とされる乱数情報が記録再生装置内の例えばＬＳＩによって生成できるので、ＰＣ内でソフトウェアによって乱数を生成するのと比較して、真正または真正乱数に近い乱数を生成することができる。したがって、乱数が固定値に置き換えられる、等のおそれを少なくできる。

【図面の簡単な説明】

【図１】

先に提案されているレコーダ、プレーヤおよびＤＶＤメディアからなるシステムを説明するためのブロック図である。

【図２】

ＰＣベースのＤＶＤメディア記録再生システムを説明するためのブロック図である。

【図３】

図２のシステムにおけるＤＶＤドライブ４およびホスト５の処理の手順を説明するための略線図である。

【図４】

図２のシステムにおける認証動作を説明するためのフローチャートである。

【図５】

この発明の一実施形態による相互認証のための構成を示すブロック図である。

【図６】

この発明の一実施形態におけるドライブの認証動作の処理の手順を説明するためのフローチャートである。

【図７】

この発明の一実施形態におけるホストの認証動作の処理の手順を説明するためのフローチャートである。

【図８】

この発明の一実施形態によるドライブとホストを組み合わせたレコーダの構成の一例をブロック図である。

【図９】

レコーダの一例の通信の手順を説明するための略線図である。

【図１０】

この発明の一実施形態によるドライブとホストを組み合わせたプレーヤの構成の一例をブロック図である。

【図１１】

プレーヤの一例の通信の手順を説明するための略線図である。

【図１２】

この発明の一実施形態によるドライブとホストを組み合わせたレコーダの構成の他の例をブロック図である。

【図１３】

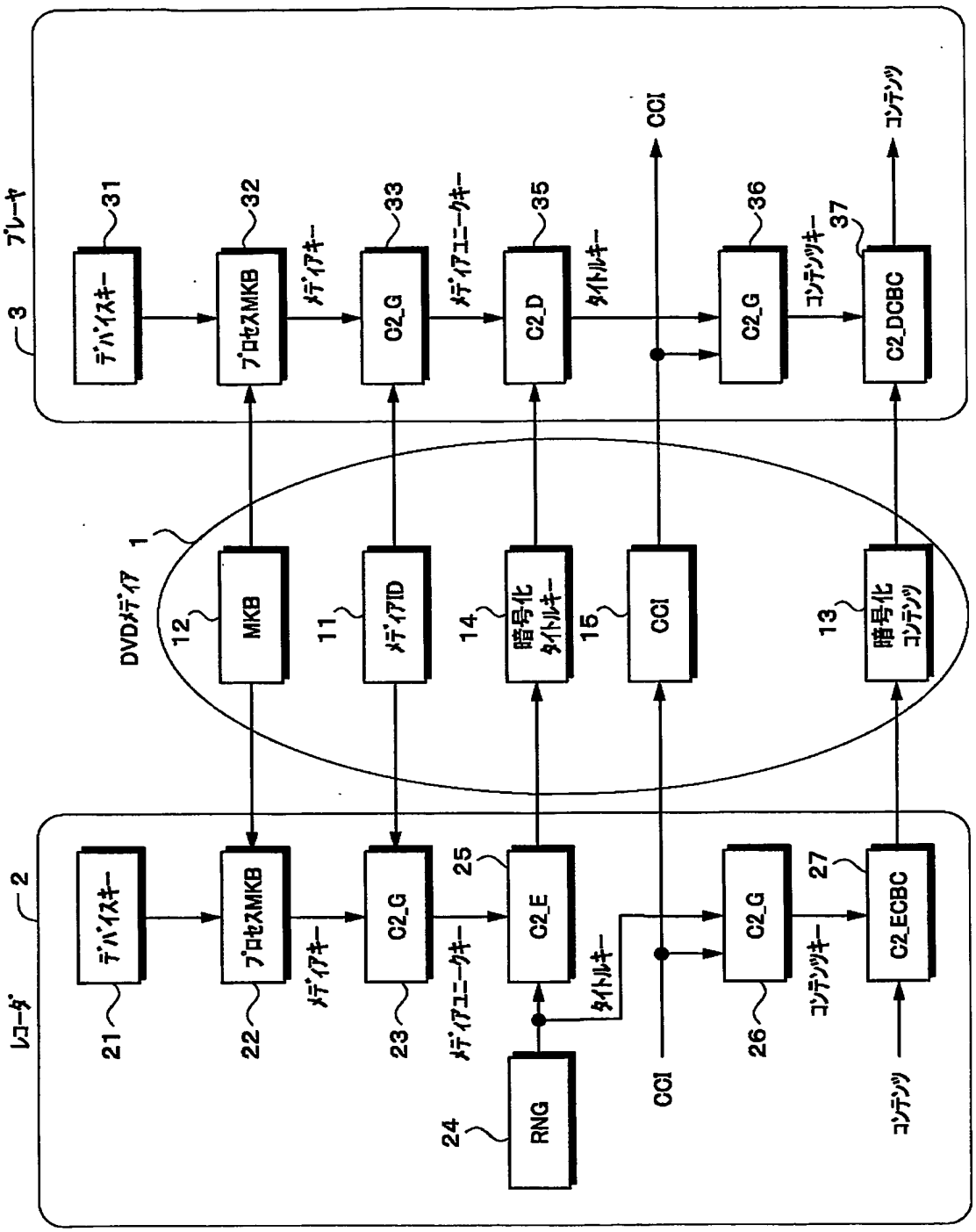
レコーダの他の例の通信の手順を説明するための略線図である。

【符号の説明】

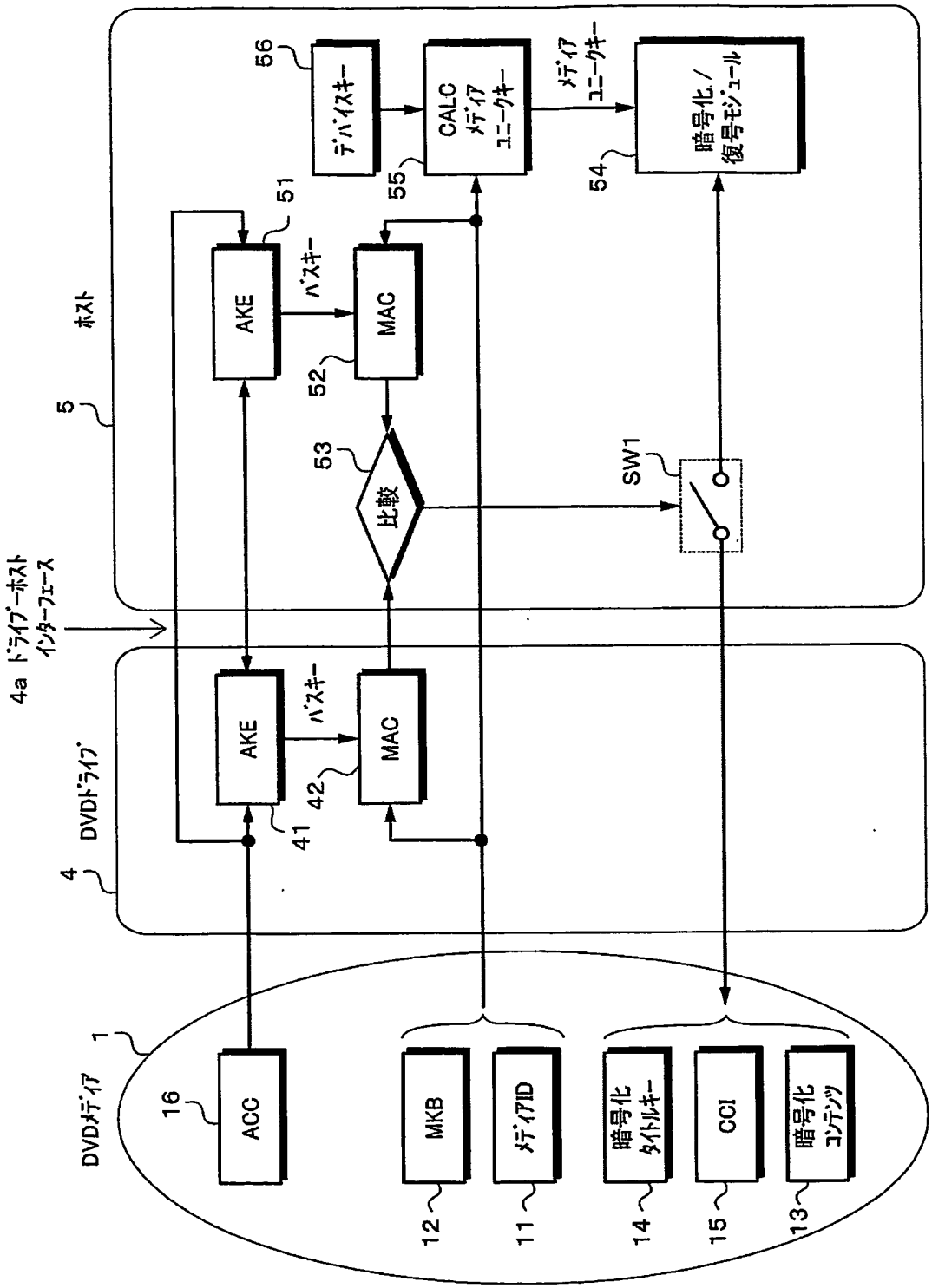
１・・・ＤＶＤメディア、２・・・レコーダ、３・・・プレーヤ、４・・・ＤＶＤドライブ、４ａ・・・インターフェース、５・・・ホスト、１１・・・メディアＩＤ、１２・・・メディアキーブロック（ＭＫＢ）、１３・・・暗号化コンテンツ、４２，５２・・・ＭＡＣ演算ブロック、４６・・・デバイスキー、４６ａ・・・デバイスキーの前半部、４７・・・ＤＥＳエンクリプタ、４８・・・メディアユニークキー演算ブロック、４９，４９ａ・・・ＤＥＳエンクリプタ、４９ｂ・・・ＤＥＳデクリプタ、５３・・・ＭＡＣを比較する比較、５４・・・暗号化／復号モジュール、５５・・・メディアユニークキー演算ブロック、１０１・・・メディア、１０２・・・ドライブ、１０３・・・ホスト、１０４・・・インターフェース、１２１・・・ドライブのデバイスキー、１２２・・・プロセスＭＫＢ、１２３，１２４，１２５・・・ドライブのＭＡＣ演算ブロック、１２６，１２７，１２８・・・ドライブの乱数発生器、１２９・・・比較、１３１・・・ホストのデバイスキー、１３２・・・プロセスＭＫＢ、１３３，１３４，１３５・・・ホストのＭＡＣ演算ブロック、１３６，１３７，１３８・・・ホストの乱数発生器、１３９・・・比較、１４１，１５４・・・Ｃ２＿Ｇ、１４２，１４４・・・ＤＥＳエンクリプタ、１４３・・・乱数発生器、１５１，１５２，１５６・・・ＤＥＳデクリプタ、１５３・・・Ｃ２＿Ｅ、１５５・・・Ｃ２＿ＥＢＣ、１５７，１５８・・・ＭＡＣ演算ブロック、１５９・・・比較

【書類名】　図面

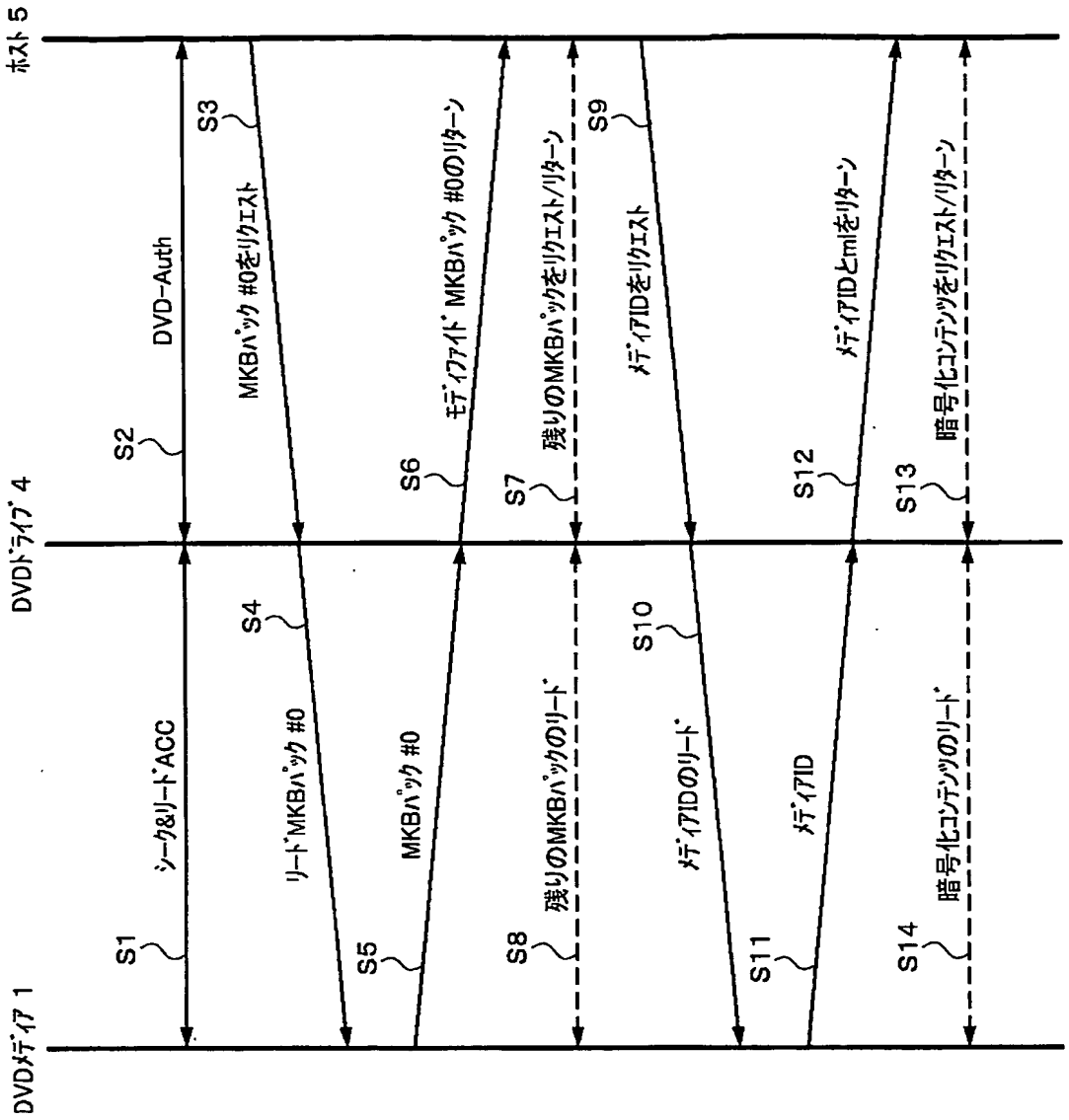
【図１】


プレーヤ
3
デバイスキー
31
プロセスMKB
32
メディアキー
C2_G
33
メディアユニークキー
C2_D
35
タイトルキー
CCI
C2_G
36
コンテンツキー
37
C2_DCBC
コンテンツ
DVDメディア
1
MKB
12
メディアID
11
暗号化タイトルキー
14
CCI
15
暗号化コンテンツ
13
レコーダ
2
デバイスキー
21
プロセスMKB
22
メディアキー
C2_G
23
メディアユニークキー
C2_E
25
タイトルキー
RNG
24
CCI
C2_G
26
コンテンツキー
27
C2_ECBC
コンテンツ

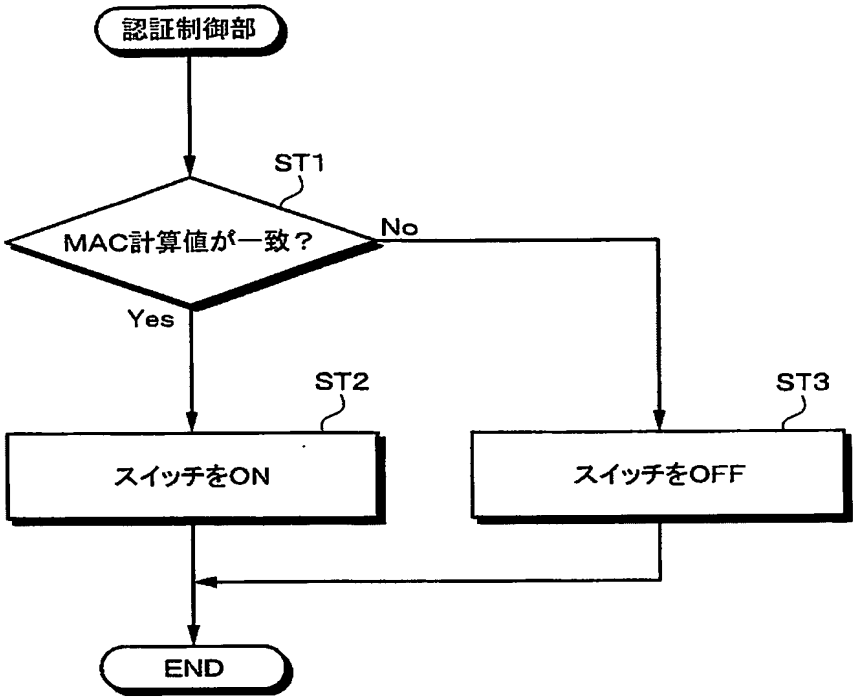
【図２】


ホスト
5
4a ドライブ－ホスト インターフェース
DVDドライブ
4
DVDメディア
1
AKE
バスキー
MAC
51
52
41
42
53
比較
SW1
56
デバイスキー
CALC メディア ユニークキー
55
メディア ユニークキー
暗号化／復号モジュール
54
16
ACC
12
MKB
11
メディアID
14
暗号化タイトルキー
15
CCI
13
暗号化コンテンツ

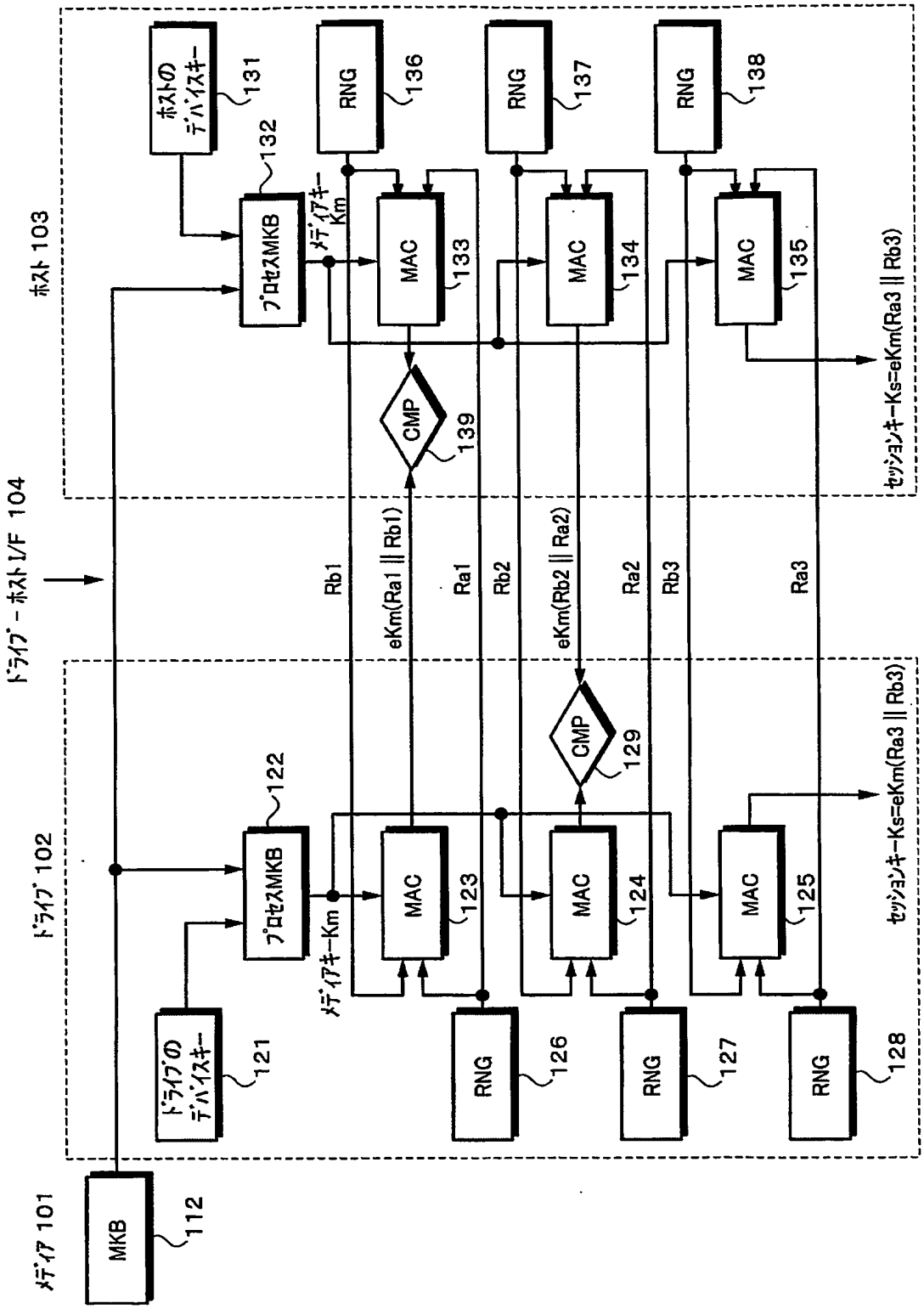
【図３】


ホスト 5
DVDドライブ 4
DVDメディア 1
S1
シーク&リード'ACC
S2
DVD-Auth
S3
MKBパック #0をリクエスト
S4
リード'MKBパック #0
S5
MKBパック #0
S6
モディファイド' MKBパック #0のリターン
S7
残りのMKBパックをリクエスト/リターン
S8
残りのMKBパックのリード'
S9
メディアIDをリクエスト
S10
メディアIDのリード'
S11
メディアID
S12
メディアIDとmlをリターン
S13
暗号化コンテンツをリクエスト/リターン
S14
暗号化コンテンツのリード'

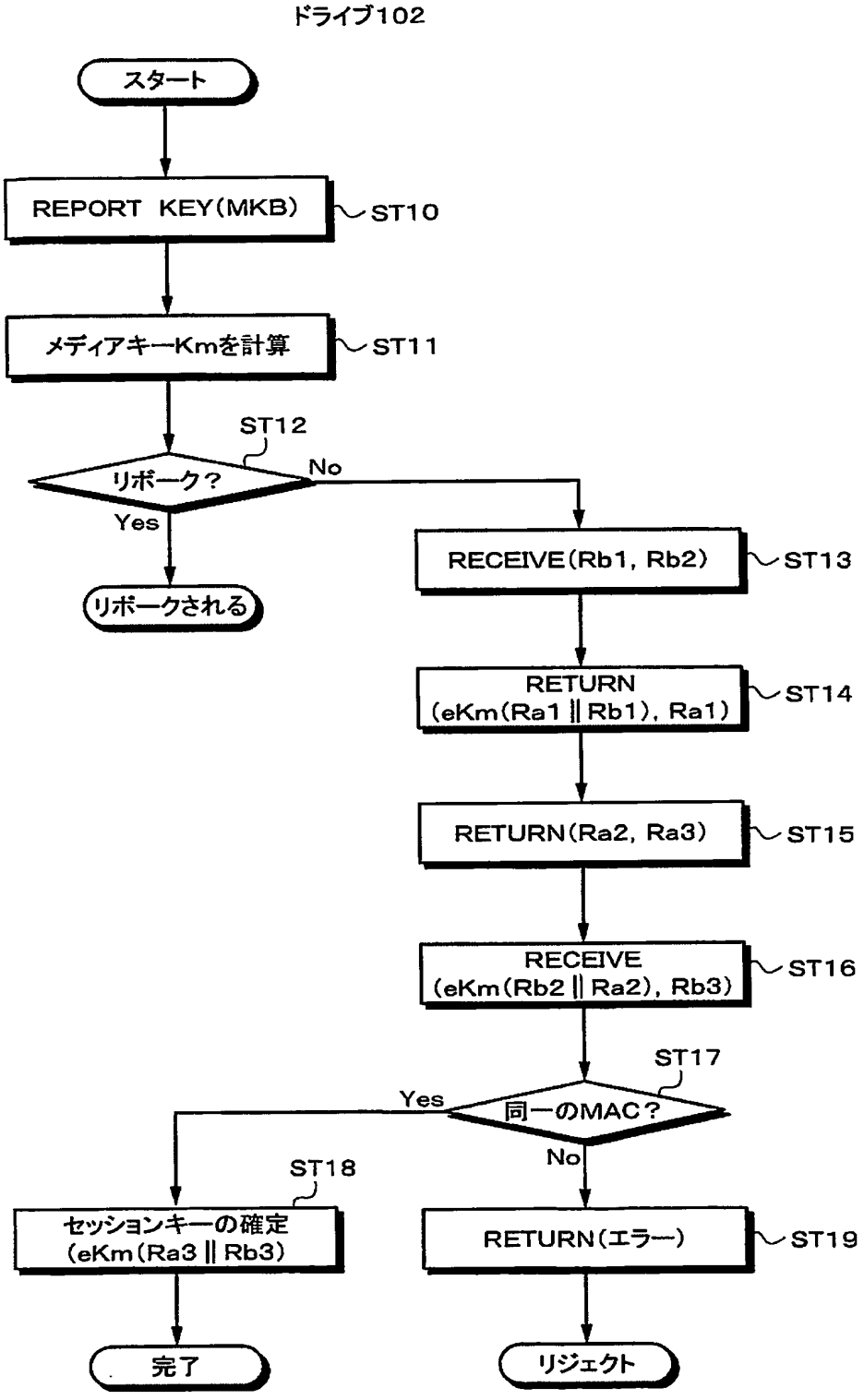
【図４】



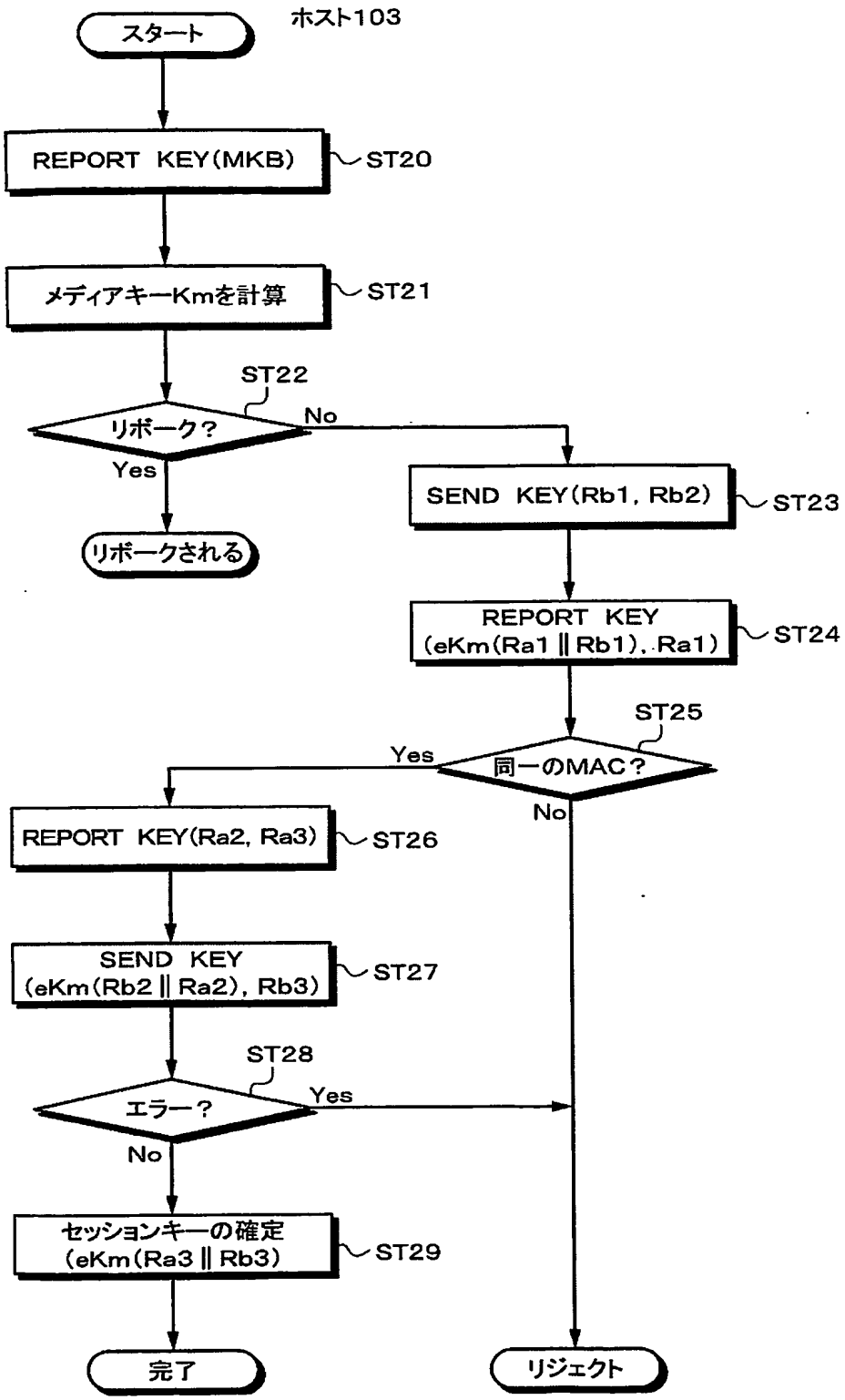
【図５】


ホスト 103
ドライブ－ホストI/F 104
ドライブ 102
メディア 101
ホストのデバイスキー
131
132
プロセスMKB
メディアキーKm
MAC
133
MAC
134
MAC
135
RNG
136
RNG
137
RNG
138
CMP
139
セッションキーKs=eKm(Ra3 || Rb3)
Rb1
eKm(Ra1 || Rb1)
Ra1
Rb2
eKm(Rb2 || Ra2)
Ra2
Rb3
Ra3
CMP
129
プロセスMKB
122
メディアキーKm
MAC
123
MAC
124
MAC
125
セッションキーKs=eKm(Ra3 || Rb3)
ドライブのデバイスキー
121
RNG
126
RNG
127
RNG
128
MKB
112

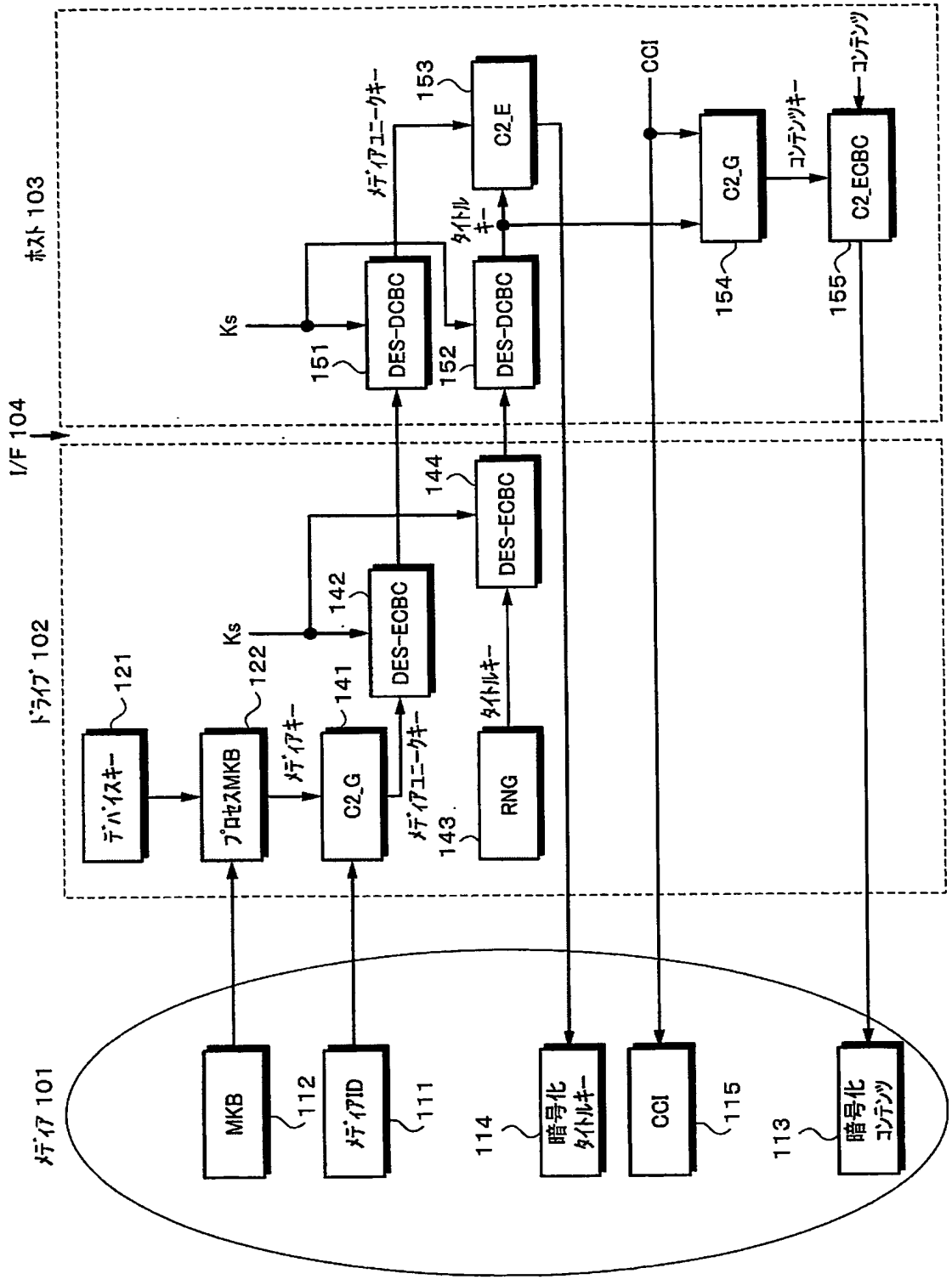
【図６】


ドライブ102
スタート
REPORT KEY(MKB)
ST10
メディアキーKmを計算
ST11
ST12
リボーク？
No
Yes
リボークされる
RECEIVE(Rb1, Rb2)
ST13
RETURN
(eKm(Ra1 ‖ Rb1), Ra1)
ST14
RETURN(Ra2, Ra3)
ST15
RECEIVE
(eKm(Rb2 ‖ Ra2), Rb3)
ST16
ST17
Yes
同一のMAC？
No
ST18
セッションキーの確定
(eKm(Ra3 ‖ Rb3)
RETURN(エラー)
ST19
完了
リジェクト

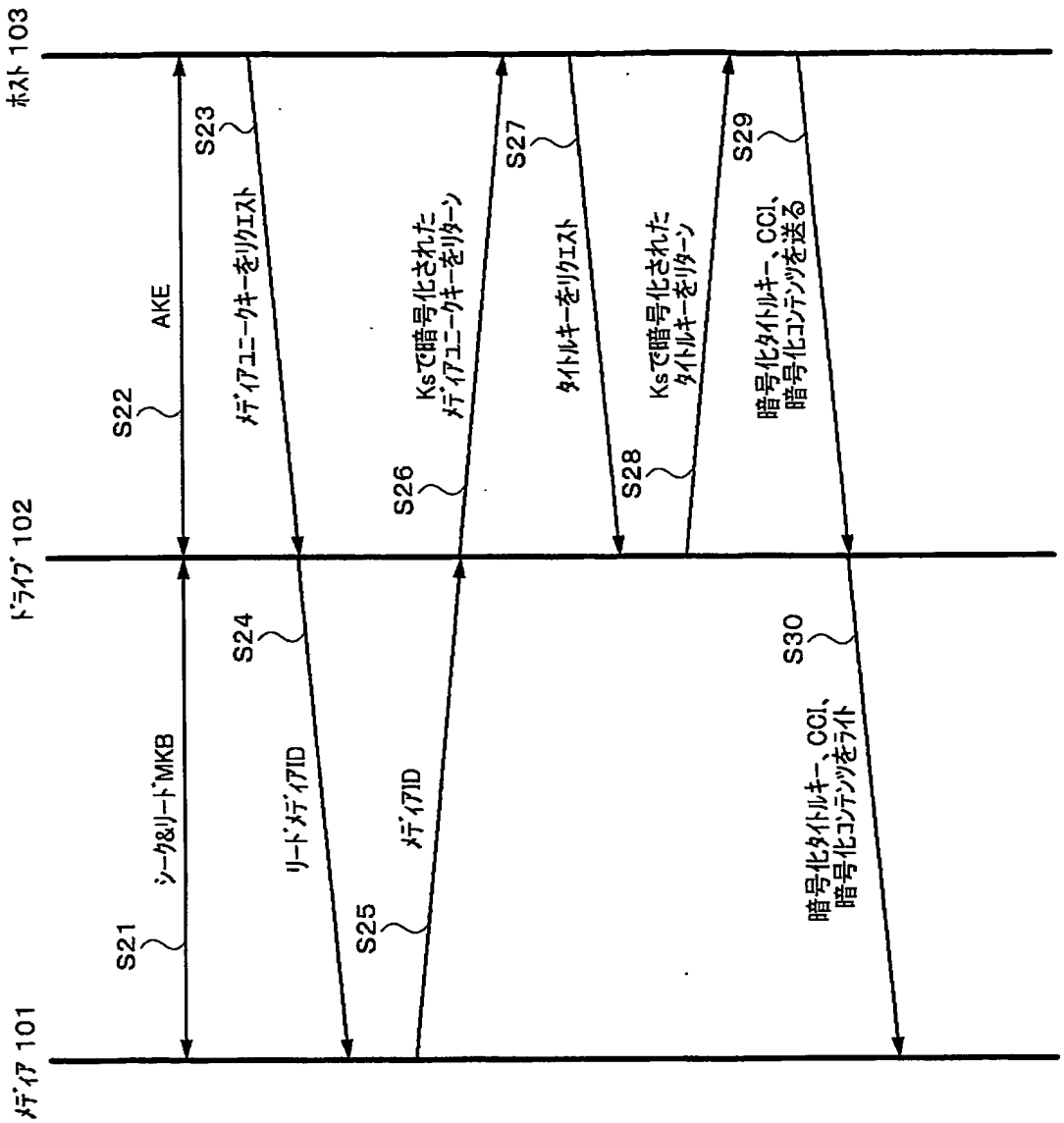
【図７】


ホスト103
スタート
REPORT KEY(MKB)
ST20
メディアキーKmを計算
ST21
ST22
リボーク？
No
Yes
リボークされる
SEND KEY(Rb1, Rb2)
ST23
REPORT KEY
(eKm(Ra1 ‖ Rb1), Ra1)
ST24
ST25
同一のMAC？
Yes
No
REPORT KEY(Ra2, Ra3)
ST26
SEND KEY
(eKm(Rb2 ‖ Ra2), Rb3)
ST27
ST28
エラー？
Yes
No
セッションキーの確定
(eKm(Ra3 ‖ Rb3)
ST29
完了
リジェクト

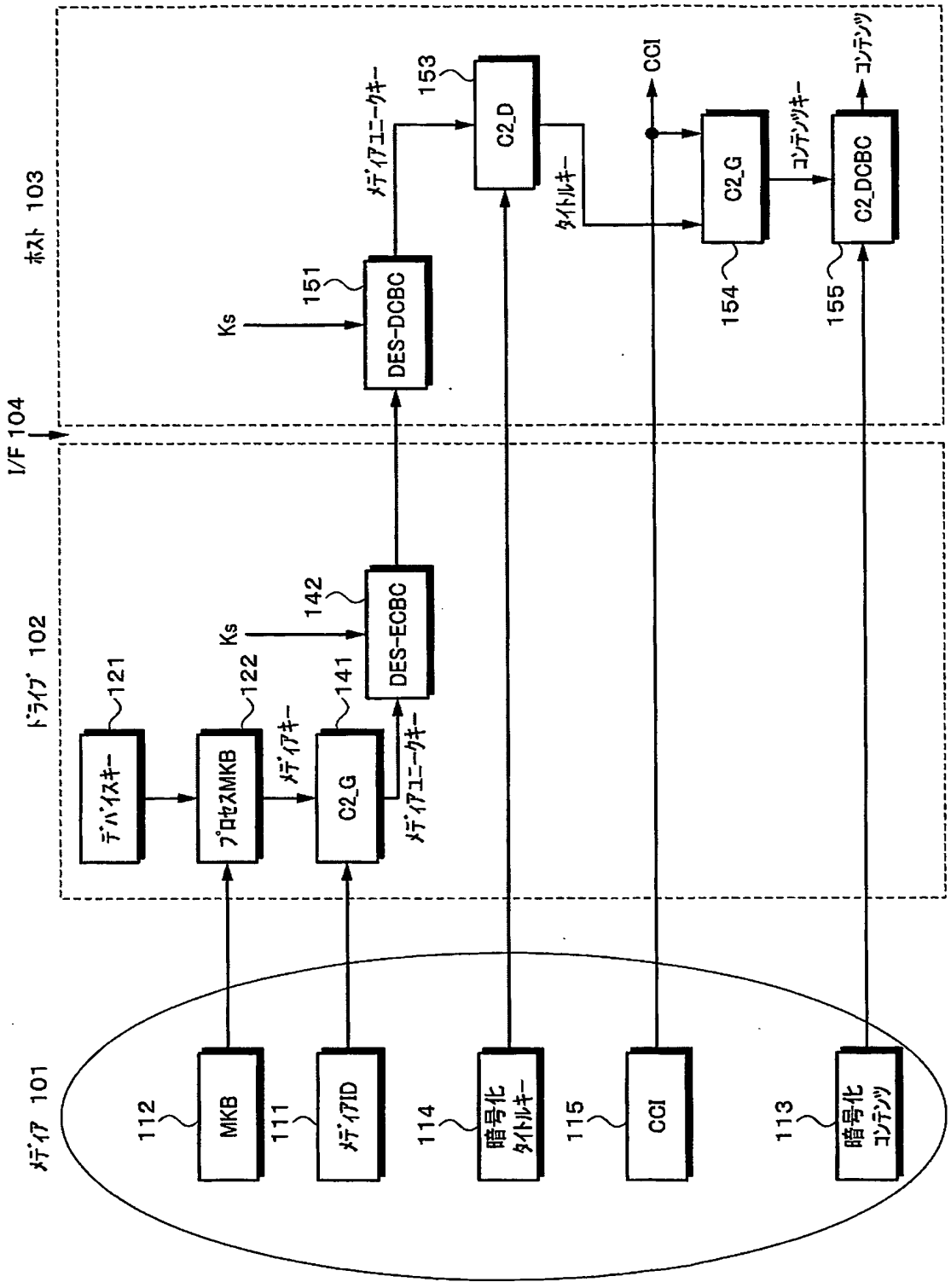
【図８】


ホスト 103
I/F 104
ドライブ 102
メディア 101
デバイスキー
121
プロセスMKB
122
メディアキー
C2_G
141
メディアユニークキー
DES-ECBC
142
Ks
DES-ECBC
144
タイトルキー
RNG
143
DES-DCBC
151
DES-DCBC
152
メディアユニークキー
C2_E
153
タイトルキー
CCI
C2_G
154
コンテンツキー
C2_ECBC
155
コンテンツ
MKB
112
メディアID
111
暗号化タイトルキー
114
CCI
115
暗号化コンテンツ
113

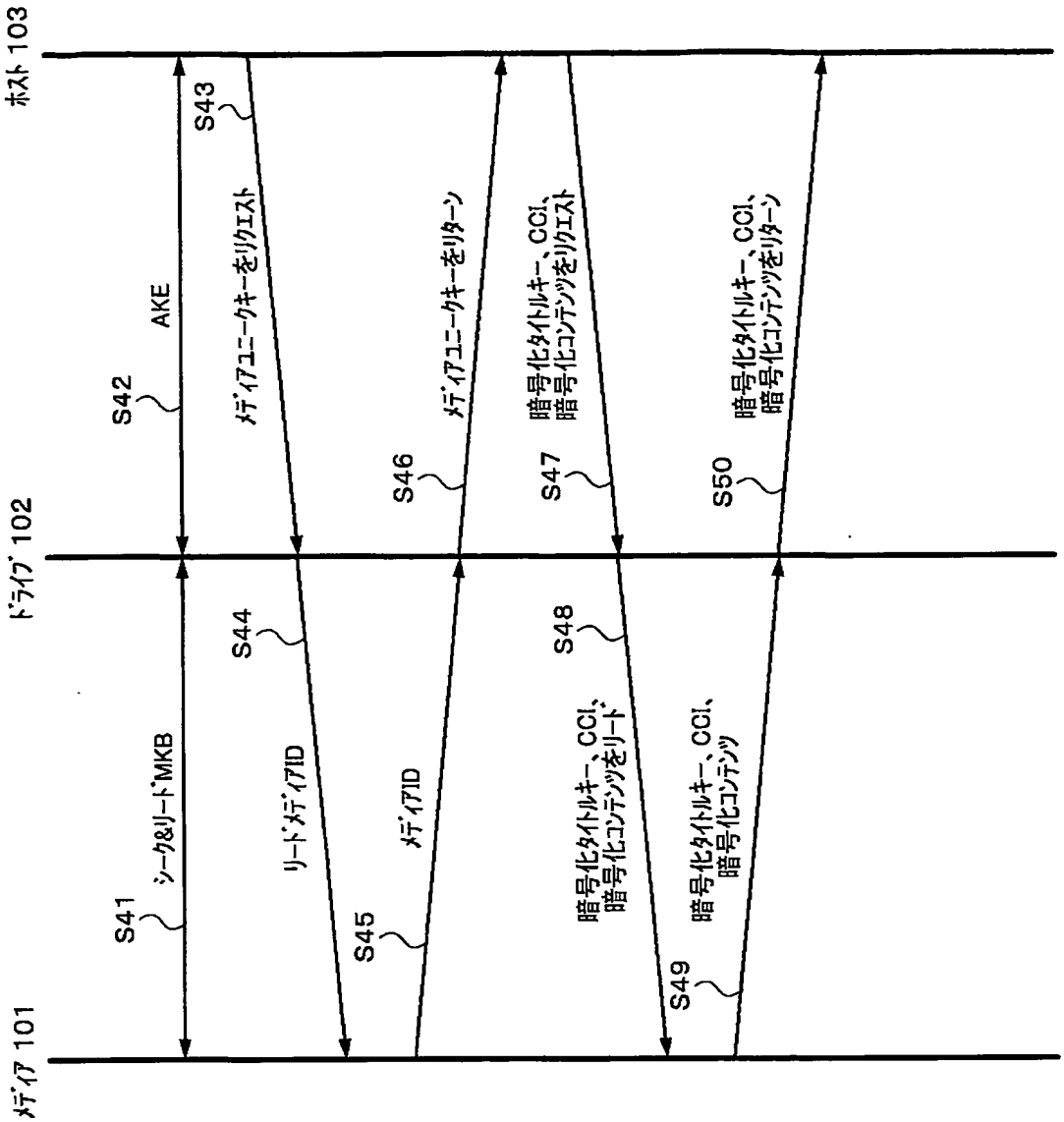
【図９】


ホスト 103
ドライブ 102
メディア 101
S21
シーク&リードMKB
S22
AKE
S23
メディアユニークキーをリクエスト
S24
リードメディアID
S25
メディアID
S26
Ksで暗号化されたメディアユニークキーをリターン
S27
タイトルキーをリクエスト
S28
Ksで暗号化されたタイトルキーをリターン
S29
暗号化タイトルキー、CCI、暗号化コンテンツを送る
S30
暗号化タイトルキー、CCI、暗号化コンテンツをライト

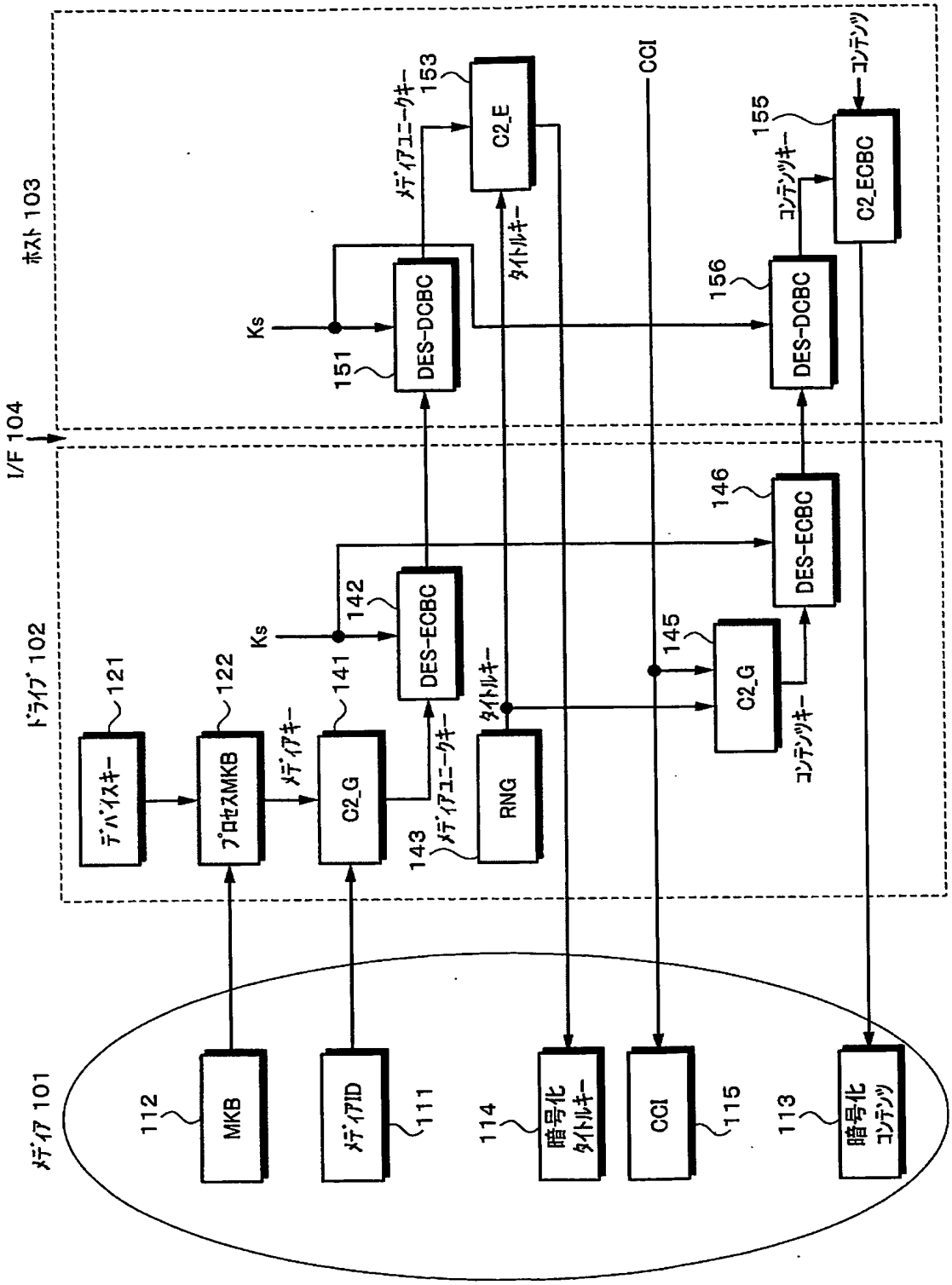
【図１０】


メディア 101
ドライブ 102
ホスト 103
I/F 104
MKB
メディアID
暗号化タイトルキー
CCI
暗号化コンテンツ
デバイスキー
プロセスMKB
C2_G
DES-ECBC
DES-DCBC
C2_D
C2_G
C2_DCBC
Ks
メディアキー
メディアユニークキー
タイトルキー
コンテンツキー
コンテンツ
111
112
113
114
115
121
122
141
142
151
153
154
155

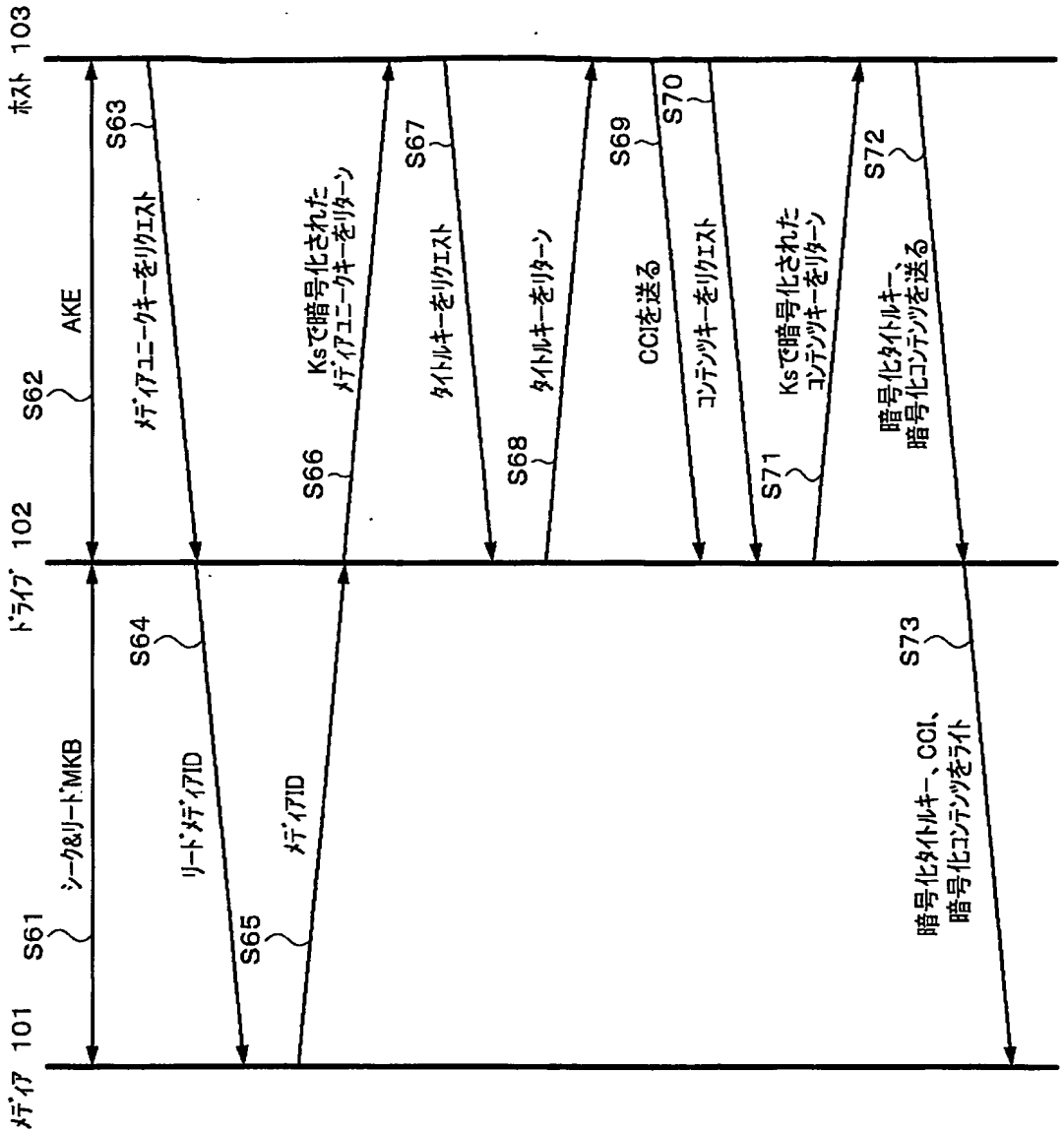
【図１１】


ホスト 103
ドライブ 102
メディア 101
S41
シーク&リード'MKB
S42
AKE
S43
メディアユニークキーをリクエスト
S44
リード'メディアID
S45
メディアID
S46
メディアユニークキーをリターン
S47
暗号化タイトルキー、CCI、暗号化コンテンツをリクエスト
S48
暗号化タイトルキー、CCI、暗号化コンテンツをリード
S49
暗号化タイトルキー、CCI、暗号化コンテンツ
S50
暗号化タイトルキー、CCI、暗号化コンテンツをリターン

【図１２】


ホスト 103
I/F 104
ドライブ 102
メディア 101
デバイスキー
121
プロセスMKB
122
メディアキー
C2_G
141
DES-ECBC
142
Ks
メディアユニークキー
143
RNG
タイトルキー
C2_G
145
DES-ECBC
146
コンテンツキー
DES-DCBC
156
C2_ECBC
155
コンテンツ
メディアユニークキー
153
C2_E
タイトルキー
Ks
DES-DCBC
151
CCI
MKB
112
メディアID
111
暗号化タイトルキー
114
CCI
115
暗号化コンテンツ
113

【図１３】


ホスト 103
ドライブ 102
メディア 101
S61
シーク&リードMKB
S62
AKE
S63
メディアユニークキーをリクエスト
S64
リードメディアID
S65
メディアID
S66
Ksで暗号化されたメディアユニークキーをリターン
S67
タイトルキーをリクエスト
S68
タイトルキーをリターン
S69
CCIを送る
S70
コンテンツキーをリクエスト
S71
Ksで暗号化されたコンテンツキーをリターン
S72
暗号化タイトルキー、暗号化コンテンツを送る
S73
暗号化タイトルキー、CCI、暗号化コンテンツをライト

【書類名】　要約書

【要約】

【課題】　著作権保護技術の安全性を高め、また、違法なドライブ等の電子機器をリボークする。

【解決手段】　プロセスＭＫＢ１２２にＭＫＢとドライブの持つデバイスキー１２１とが入力され、ドライブがリボーク処理され、プロセスＭＫＢ１３２によってホスト１０３がリボーク処理される。ＭＡＣ演算ブロック１２３および１３３が演算したＭＡＣ値がホスト１０３内において比較され、二つの値が同一と判定されると、ホスト１０３によるドライブ１０２の認証が成功したことになる。ホスト１０３のＭＡＣ演算ブロック１３４および１２４が演算したＭＡＣ値がドライブ１０２内において比較され、二つの値が同一と判定されると、ドライブ１０２によるホスト１０３の認証が成功したことになる。相互認証が成功すると、ＭＡＣ演算ブロック１２５および１３５によって、共通のセッションキーが生成される。

【選択図】　図５

特願２００３－００６９１５

出　願　人　履　歴　情　報

識別番号　　［０００００２１８５］

１．変更年月日　　１９９０年　８月３０日
［変更理由］　　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社